# MASTER ACCOUNT AND SERVICE TERMS
# ГЕНЕРАЛЬНІ УМОВИ ОБСЛУГОВУВАННЯ РАХУНКУ ТА НАДАННЯ ПОСЛУГ

**1. Introduction**

**1.1** The Terms (as defined in 1.4 below) apply to each bank account (an "Account") opened using a Customer Activation Form signed by the Customer or in any other manner acceptable to the Bank, and are binding on the Customer and the direct or indirect bank subsidiary of Citigroup Inc. that holds the Account ("Bank"). If the Bank has more than one branch, then "Bank" means the branch where the Account is held or the branch that performs the Service (as defined below). In addition, the Terms apply to products and services provided by the Bank that are account-related and to any other product or service which is expressed to be subject to the MAST (or any predecessor account terms and conditions of the Bank) (a "Service"). These Master Account and Service Terms (the "MAST") include the Confidentiality and Data Privacy Conditions referred to in Section 9 hereof ("CDPC"), which also apply to Trade Transactions (as defined in the CDPC) to the extent provided in the CDPC.

**1.2.** The MAST are supplemented and/or amended for Accounts and Services provided in certain countries or territories by local conditions (the "Local Conditions") that will be supplied to the Customer by the Bank and will be binding on the Customer and the Bank.

**1.3.** If there is a conflict between the MAST and any Local Conditions, the Local Conditions prevail; and if there is a conflict between the MAST or any Local Conditions and any agreement or other conditions relating to a Service including any Service-related materials such as user guides (a "Service Agreement"), that Service Agreement prevails.

**1. Вступ**

**1.1** Умови (як визначено нижче у розділі 1.4) застосовуються до кожного банківського рахунку («Рахунок»), що відкритий відповідно до Форми активації клієнта чи у будь-який інший прийнятний для Банку спосіб, і є обов'язковими для Клієнта та прямої чи непрямої банківської дочірньої компанії Citigroup Inc., яка обслуговує такий Рахунок («Банк»). Якщо Банк має більше, ніж одне відділення, тоді «Банк» означає відділення, в якому Рахунок обслуговується, чи відділення, яке надає Послуги (як визначено нижче). Крім того, ці Умови застосовуються до продукції та послуг, наданих Банком стосовно рахунку, та до будь-якої іншої продукції чи послуг, які підпорядковані умовам MAST (чи будь-яким попереднім умовам Банку, що регулюють обслуговування рахунку) («Послуга»). Ці Генеральні умови обслуговування рахунку та надання послуг "Master Account and Service Terms" (ГУ), включають Умови конфіденційності та секретності даних "Confidentiality and Data Privacy Conditions" (УК), зазначені в Розділі 9, які також застосовуються до Комерційних операцій (як визначено в УК) в межах, передбачених УК.

**1.2.** Умови ГУ, доповнені та/або змінені для Рахунків та Послуг, що надаються у певних країнах чи територіях, відповідно до місцевих умов («Місцеві умови»), надаються Клієнту Банком і є обов'язковими для Клієнта та Банку.

**1.3.** У разі виникнення протиріч між умовами ГУ та Місцевими умовами, переважну силу мають Місцеві умови; у разі виникнення протиріч між умовами ГУ чи будь-якими Місцевими умовами та будь-якою угодою чи іншими умовами, пов'язаними з Послугами, включаючи будь-які документи, що стосуються Послуг, такі як інструкції користувача («Угода про послуги»), переважну силу має Угода про послуги.

**1.4.** When used herein, the term "Terms" refers collectively to the MAST, the Local Conditions and the Service Agreements.

**2. Authority**

The Bank may rely on the authority of each person designated in writing (in a form acceptable to the Bank) by the Customer to send Communications (defined below) or do any other thing until the Bank has received written notice acceptable to it of any change from a duly authorized person and the Bank has had a reasonable time to act (after which time it may rely on the change).

**3. Communications**

**3.1.** Each of the Customer and the Bank will comply with certain agreed security procedures (the "Procedures") designed to authenticate the Customer's log-on to the Bank's connectivity channels and to verify the origination of communications between them such as enquiries, data and other information exchanges, advices, transactional instructions, and account management instructions (each a "Communication"). Depending upon the method of Communication used by the Customer, the Procedures may constitute one or more of the following measures: unique transaction identifier, digital signatures, encryption algorithms or other codes, multifactor authentication, user entitlements, schedule validation or such other measures as in use for the Communications method agreed to by the Customer. Procedures for Communications involving MIFTs (as defined in 3.4 below) are provided in connection with the use of that service.

**3.2.** The Bank is not obliged to do anything other than what is contained in the Procedures to establish the authority or identity of the person sending a Communication and may rely upon the authority and identity of such person if the Bank complies with the Procedures. The Bank is not responsible for errors or omissions made by the Customer or the duplication of any Communication by the Customer and may act on any Communication by reference to a bank identification or account number only, even if a bank or account name is provided. The Bank will promptly notify the Customer (by telephone if appropriate) if a Communication is not acted upon for any reason.

**3.3.** If the Customer requests the Bank to recall, cancel or amend a Communication, the Bank will use its reasonable efforts to comply and the Customer shall be responsible for all costs, losses and other expenses related thereto.

**3.4.** If the Bank acts on a manually initiated funds transfer ("MIFT") instruction in accordance with the Procedures, the Customer will be responsible for any costs, losses and other expenses related thereto.

**4. Credits and Debits**

**4.1.** The Bank is not obliged to make a credit to an Account before receipt by the Bank of a corresponding and final payment in cleared funds. If the Bank makes a credit before such receipt, the Bank may reverse all or part of the credit (including any interest thereon), make an appropriate entry to the Account and require repayment of an amount corresponding to such credit if it has been withdrawn.

**1.4.** Посилання на термін «Умови» вважати посиланням на умови ГУ, Місцеві умови та умови Угод про послуги.

**2. Повноваження**

Банк може прийняти повноваження кожної особи, призначеної Клієнтом у письмовій формі (у формі, прийнятній для Банку) для відправлення Повідомлень (визначення яких наводиться нижче) та здійснювати будь-які інші операції, до отримання Банком належного письмового повідомлення про будь-які зміни від належно уповноваженої особи, після закінчення обґрунтованого періоду часу, необхідного Банку для вчинення відповідних дій, Банк може прийняти таку зміну.

**3.** Повідомлення

**3.1.** Клієнт і Банк зобов'язуються дотримуватися певних узгоджених процедур безпеки («Процедури»), призначених для перевірки автентичності під час входу Клієнта до каналів зв'язку Банку та перевірки походження повідомлень між ними, таких як запити, дані та інший обмін інформацією, рекомендації, транзакційні інструкції та інструкції щодо управління рахунком (разом – «Повідомлення»). Залежно від методу Обміну інформацією, що використовується Клієнтом, Процедури можуть складати один або декілька наступних заходів: унікальний операційний ідентифікатор, цифрові підписи, алгоритми шифрування чи інші коди, багатофакторна ідентифікація, найменування користувача, перевірка графіка чи інші подібні заходи, які застосовуються для методу обміну Повідомленнями, погодженого Клієнтом. Процедури щодо Обміну інформацією для послуги MIFT (як визначено нижче в пункті 3.4) застосовуються у зв'язку з використанням цієї послуги.

**3.2.** Банк не зобов'язаний вчиняти будь-які інші дій, крім тих, що передбачені Процедурами, для встановлення повноважень та особи відправника Повідомлення і може покладатися на повноваження та відомості про таку особу, якщо Банк дотримується Процедур. Банк не несе відповідальності за помилки чи упущення Клієнта або за дублювання будь-якого Повідомлення, і може діяти на підставі будь-якого Повідомлення лише через посилання на ідентифікацію банку чи зазначення номеру рахунку, навіть якщо зазначено найменування банку чи рахунку. Банк відразу повинен повідомити Клієнта (телефоном, якщо це необхідно), якщо Банком не були вчинені дії за Повідомленням з будь-якої причини.

**3.3.** Якщо Клієнт вимагає від Банку відкликати, скасувати чи змінити Повідомлення, Банк буде використовувати всі розумні зусилля для цього, а Клієнт нестиме відповідальність за усі витрати, збитки та інші видатки, пов'язані з цим.

**3.4.** Якщо Банк діє на підставі інструкції що вимагає ручного відправлення («MIFT», manually initiated funds transfer) Клієнт нестиме відповідальність за будь-які витрати, збитки та інші видатки, пов'язані з цим, за умови дотримання Банком Процедур.

**4. Зарахування коштів на Рахунок та списання коштів з Рахунку**

**4.1.** Банк не зобов'язаний зараховувати на Рахунок будь-який платіж до отримання ним відповідного підтвердження. Якщо Банк зараховує на Рахунок будь-яку суму до отримання такого підтвердження, Банк може анулювати зарахування всієї суми або її частини (включаючи всі нараховані проценти на таку суму), внести відповідний запис до Рахунку та вимагати компенсації

суми, яка відповідає такому надходженню, якщо вона була списана.

**4.2.** The Bank may, but is not obliged to, make a debit to an Account, whether based upon payment instructions from the Customer or in accordance with the Terms that might result in or increase a debit balance. If the total amount of debits to an Account at any time would exceed the immediately available funds credited to the Account, and any available credit lines that may be utilized for such purpose, the Bank may decide which debits it will make (in whole or in part and in the order it selects).

**4.2.** Банк може, але не зобов'язаний, списувати з Рахунку будь-яку суму на основі платіжних інструкцій від Клієнта або відповідно до Умов, якщо така проводка приведе до утворення або збільшення дебетового сальдо. Якщо загальна сума, списана з Рахунку в будь-який момент приведе до перевищення суми зарахованих на Рахунок коштів, що надаються у негайне розпорядження і будь-яких доступних зарахувань, які можуть бути використані для такої мети, Банк може прийняти рішення про те, які кошти списувати з Рахунку (всі чи їх частину і в обраному ним порядку).

**4.3.** Unless otherwise provided in an agreement signed by the Bank and the Customer, the Bank may at any time cancel any extensions of credit with respect to any Account or Service. The Customer will transfer to the Bank on closure of an Account and otherwise on demand from the Bank sufficient immediately available funds to cover any debit balance on an Account or any other utilized extensions of credit and any interest, fees and other amounts owed.

**4.3.** Якщо інше не зазначено в договорі, укладеному між Банком та Клієнтом, Банк може у будь-який час анулювати будь-які операції по зарахуванню коштів по відношенню до будь-якого Рахунку чи Послуг. В разі закриття Рахунку чи за інших обставин за вимогою Банку, Клієнт перекаже до Банку кошти, що надаються у негайне розпорядження, в сумі, яка є достатньою для покриття будь-якого дебетового сальдо на Рахунку чи будь-якої іншої суми, що зарахована на Рахунок, а також будь-яких процентів, зборів та інших сум, що підлягають оплаті.

**5. Checks and Payment Instruments**
The Customer will make reasonable efforts to avoid any fraud, loss, theft, misuse or dishonor in respect of checks, payment instruments and related materials. The Customer will promptly notify the Bank in writing of the loss or theft of any check or payment instrument and will return to the Bank or destroy any unused checks, payment instruments and related materials when the relevant Account is closed.

**5. Чеки та платіжні документи**
Клієнт повинен докладати належних зусиль, щоб уникнути будь-якого шахрайства, втрати, крадіжки, зловживання або відмови в оплаті чеків, платіжних документів та пов'язаних з ними матеріалів. Клієнт повинен відразу повідомити Банк письмово про втрату чи крадіжку будь-якого чеку чи платіжного документу і повинен повернути Банку або знищити будь-які невикористані чеки, платіжні документи і пов'язані з ними матеріали, коли відповідний Рахунок закрито.

**6. Statements and Advices**
The Customer shall notify the Bank in writing of anything incorrect in a statement or advice promptly and in any case within thirty (30) days from the date on which the statement or advice is sent in writing or made available to the Customer. Nothing herein is intended to prevent the Customer from notifying the Bank of any errors or corrections beyond such time, provided that the Bank shall not be responsible for any losses caused by such delay in notification.

**6. Виписки і авізо**
Клієнт повинен повідомити Банк у письмовій формі про будь-які помилки у виписках чи авізо відразу і у будь-якому випадку протягом тридцяти (30) днів з дати, від якої виписки чи авізо були надіслані в письмовій формі чи були надані Клієнтові. Ніщо не зазначене тут не повинно перешкоджати Клієнтові повідомити Банк про будь-які помилки чи виправлення і поза встановленим терміном, за умови, що Банк не нестиме відповідальності за будь-які збитки, спричинені такою затримкою у повідомленні.

**7. Interest, Fees and Taxes**
**7.1.** The Customer shall pay to the Bank all fees, interest and other amounts that apply to the Accounts and Services. Unless otherwise agreed in writing, the Bank may modify any fees, interest rates and other amounts at any time (but subject to any legal requirement as to notice).

**7. Проценти, збори та податки**
7.1. Клієнт повинен сплатити Банку всі збори, проценти та інші кошти, що стосуються Рахунків та Послуг. Якщо не погоджено інше в письмовій формі, Банк може змінювати будь-які збори, процентні ставки та інші суми у будь-який час (але з урахуванням законодавчих вимог щодо надання повідомлення).

**7.2.** All such fees, interest and other amounts are payable to the Bank without deduction for taxes or amounts of a similar nature ("Taxes"), which are the responsibility of the Customer. If any such Taxes are paid by the Bank or any of its affiliates, the Customer shall promptly reimburse the Bank for such payment.

**7.2.** Усі такі збори, проценти та інші суми підлягають сплаті Банку без вирахування податків чи сум подібного характеру («Податки»), за сплату яких несе відповідальність Клієнт. Якщо такі Податки сплачуються Банком або будь-якою з його філій, Клієнт повинен відразу відшкодувати Банку такий платіж.

**7.3.** The Customer is responsible for all Taxes on earned interest and other payments made by the Bank to the Customer. If required by any applicable Government Requirement (as defined below), the Bank shall deduct or withhold for or on account of Taxes from any such payments to the Customer. The Bank shall timely pay the full amount withheld to the relevant governmental authority in accordance with such Government Requirement. The Bank shall notify the Customer of any such withholding as soon as reasonably practicable.

**7.4.** The Customer shall notify the Bank in writing within 30 days of any change that affects the Customer's tax status pursuant to any Government Requirement (e.g., a change in the Customer's country of residence or in its legal entity classification, or if it ceases to be or becomes a financial institution).

**7.5.** Unless otherwise agreed in writing, the Bank may debit any Account for fees, interest or other amounts due to the Bank.

**8. Performance**

**8.1.** The Bank will perform in good faith and with reasonable care, as determined in accordance with the standards and practices of the banking industry. In connection with its provision of Services under the Terms, the Bank may use any communications, clearing or payment system, intermediary bank or other entity (each, a "System") and Services are subject to the rules and regulations of any such System.

**8.2.** Neither the Customer nor the Bank shall have any liability for any special or punitive damages, indirect, incidental or consequential losses or damages, or any loss of profit, goodwill or business opportunity, whether or not the relevant loss or damage was foreseeable or contemplated, even if one party advised the other of the possibility of such loss or damage.

**8.3** Any obligation of the Bank with respect to an Account is (i) subject to the Government Requirements of the country or territory in which the Bank is located, and (ii) is enforceable only at and against the Bank, which is the sole place of payment and not at or against another branch or affiliate of the Bank. The Bank is only obliged to make payments in respect of an Account in the currency in which the Account is denominated at the time of such payment or as may otherwise be required by Government Requirement (as defined below).

**7.3.** Клієнт несе відповідальність за сплату усіх Податків на отримані проценти та інші платежі, здійсненні Банком на користь Клієнта. Якщо це вимагається чинною вимогою законодавства (як визначено нижче), Банк повинен списати чи утримати кошти з Рахунку на суму Податків з будь-яких таких платежів Клієнту. Банк повинен своєчасно сплачувати повну суму, що утримується на користь відповідного державного органу відповідно до вимог законодавства. Банк повинен повідомити Клієнта про будь-яке таке утримання у найкоротші можливі строки.

**7.4.** Клієнт повинен повідомити Банк в письмовій формі протягом 30 днів про будь-які зміни, які стосуються статусу платника податків Клієнта відповідно до вимог законодавства (наприклад, зміна країни проживання/місцезнаходження Клієнта чи зміна в класифікації юридичної особи, або якщо він перестає бути або стає фінансовою установою).

**7.5.** Якщо інше погоджено письмово, Банк може виконати дебетування будь-якого Рахунку на суму зборів, процентів чи інші суми коштів, заборговані Банку.

**8. Виконання обов'язків**

**8.1.** Банк буде сумлінно виконувати свої обов'язки з належною обачливістю, як це визначено відповідно до прийнятних норм і практики у банківській галузі. У зв'язку з наданням своїх Послуг відповідно до Умов, Банк має право використовувати будь-які засоби зв'язку, клірингову або платіжну систему, банки-посередники чи інші організації (кожен окремо «Система») та Послуги, які регулюються правилами та положеннями будь-якої такої Системи.

**8.2.** Клієнт і Банк не несуть відповідальності за будь-які спеціальну чи штрафну шкоду, непрямі, випадкові чи наслідкові збитки і шкоду чи за будь-яку упущену вигоду, зіпсовану ділову репутацію чи втрачені можливості для бізнесу, незалежно від того, чи були вони передбачуваними чи очікуваними, навіть якщо одна сторона повідомляла іншій про можливість настання таких збитків чи шкоди.

**8.3** Будь-яке зобов'язання Банку стосовно Рахунку (а) підпорядковується нормам законодавства країни чи території, де знаходиться Банк, і (б) поширюється тільки на і щодо Банку, який є єдиним місцем платежу, а не щодо іншої філії чи афілійованої особи Банку. Банк зобов'язаний проводити платежі за Рахунком у валюті, в якій Рахунок відкритий на час здійснення такого платежу, якщо інше не передбачено чинним законодавством (як визначено нижче).

**8.4.** Neither the Customer nor the Bank will be responsible for any failure to perform any of its obligations with respect to any Account or Service (including, with respect to the Bank, a request for payment or transfer from an Account) if such performance would result in a breach by it, its related branches, affiliates, or the Systems, of any Government Requirement or if its performance is prevented, hindered or delayed by a Force Majeure Event; in such case its obligations will be suspended for so long as the Force Majeure Event continues (and, in the case of the Bank, no other branch or affiliate shall become liable). Neither the Bank nor any of its related branches or affiliates will be responsible for any action taken to comply with economic sanctions or Government Requirement (and no other branch or affiliate shall become liable). "Force Majeure Event" means any event due to any cause beyond the control of the relevant party, such as restrictions on convertibility or transferability, requisitions, involuntary transfers, unavailability of any System, sabotage, fire, flood, explosion, acts of God, economic sanctions, Government Requirement, civil commotion, strikes or industrial action of any kind, riots, insurrection, war or acts of government or similar institutions. "Government Requirement" means any applicable law or regulation, any requirement or decree of a legal, governmental, regulatory or similar authority, or an agreement entered into by the Bank and any governmental authority or between two or more governmental authorities (such law, regulation or authority may be domestic or foreign).

**8.4.** Ні Клієнт, ні Банк не несуть відповідальності за невиконання будь-якого свого обов'язку стосовно будь-якого Рахунку чи Послуги, (включаючи ті, що стосуються Банку, вимоги платежу чи переведення коштів з Рахунку), якщо виконання таких дій спричинить порушення вимог законодавства ним, відповідними філіями, афілійованими особами чи Системами, чи якщо такому виконанню перешкоджають, ускладнюють чи затримують виконання форс-мажорні обставини в такому випадку виконання зобов'язання призупиняється на весь час дії такої форс-мажорної обставини (і, якщо це стосується Банку, від такої відповідальності звільняється будь-яка його філія чи афілійована особа). Ні Банк, ні будь-яка з його філій чи афілійованих осіб не нестиме відповідальності за будь-які дії з метою дотримання економічних санкцій чи вимог законодавства (і будь-яка інша філія чи афілійована особа не нестимуть відповідальності). «Форс-мажорна обставина» означає будь-яку обставину поза сферою контролю відповідної сторони, такі як обмеження можливості обміну валюти або переказу валюти, реквізиції, примусові трансферти, недоступність будь-якої Системи, диверсія, пожежі, повені, вибухи, стихійні лиха, економічні санкції, вимога законодавства, громадські заворушення, страйки та будь-які трудові конфлікти, бунти, повстання, війни чи дії уряду або подібних інституцій. «Вимога законодавства» означає будь-яке чинне законодавство або норми, будь-яку вимогу або декрет законодавчого, урядового, регуляторного або аналогічного органу влади, чи угоду, укладену між Банком та будь-яким державним органом чи між двома чи більше органами влади (таке законодавство чи органи влади можуть бути локальними чи іноземними).

**8.5.** Without prejudice to any other provision in the Terms, this Section 8 applies to all rights and obligations of the Customer and the Bank in respect of the activities contemplated by the Terms, including, without limitation, any claims arising in connection with such activities that may be made against either party, whether arising from breach of contract, tortious or similar acts, or otherwise.

**8.5.** Без обмеження щодо будь-яких інших положень в Умовах, цей Розділ 8 застосовується до усіх прав і обов'язків Клієнта і Банку стосовно діяльності, передбаченої Умовами, включаючи, але не обмежуючись, будь-які претензії, що виникають у зв'язку з такою діяльністю, які можуть виникнути проти іншої сторони, в результаті порушення контракту, деліктних чи схожих дій або іншим чином.

**9. Customer Information**
Responsibilities of each party relating to the privacy and confidentiality of information are set forth in the CDPC, which are incorporated herein by reference.

**9. Інформація Клієнта**
Обов'язки кожної сторони, пов'язані з конфіденційністю інформації, викладені в умовах УК, які є частиною цих ГУ.

**10. Closing an Account; Termination**
**10.1.** Subject to any requirements of applicable law or unless otherwise agreed in writing, the Bank or the Customer may close an Account or terminate all or part of any Service upon written notice.

**10. Закриття Рахунку. Припинення дії ГУ**
**10.1.** Відповідно до будь-яких вимог чинного законодавства, або якщо інше не погоджено письмово, Банк чи Клієнт можуть закрити Рахунок або припинити надання будь-яких Послуг повністю або частково шляхом надсилання письмового повідомлення.

**10.2.** On closure of an Account, the Bank will, subject to the Terms, pay to the Customer any final cleared funds standing to the credit of the Account (and any interest due) as at the time the Account is closed.

**10.2.** При закритті Рахунку Банк, як визначено Умовами, сплачує Клієнту будь-які залишки коштів, що зараховані на Рахунок (разом із відсотками, що підлягають виплаті) на момент закриття Рахунку.

**11. General**

**11.1.** Neither the Customer nor the Bank may assign or transfer any of its rights or obligations under the Terms without the other party's prior written consent, which will not be unreasonably withheld or delayed, provided that the Bank may make such an assignment or transfer to a branch or affiliate if it does not materially adversely affect the provision of services to the Customer. The Bank shall provide notice of any such assignment or transfer.

**11.2.** If any provision of the Terms is or becomes illegal, invalid or unenforceable under any applicable law, the remaining provisions of the Terms will remain in full force and effect (as will that provision under any other law).

**11.3.** No failure or delay of the Customer or the Bank in exercising any right or remedy under the Terms will constitute a waiver of that right. Any waiver of any right will be limited to the specific instance.

**11.4.** The Customer and the Bank consent to telephonic or electronic monitoring or recording for security and quality of service purposes and agree that either party may produce telephonic or electronic recordings or computer records as evidence in any proceedings brought in connection with the Terms.

**11.5.** Written notice shall be effective (i) if delivered to the Customer's principal business address specified in the Customer Activation Form or to the Bank's address on the most recent statement for the relevant Account or (ii) if sent to such other address as one party may notify the other party in writing, including an address for notices to be sent electronically. Notices shall be in English unless otherwise agreed or required by local law.

**11.6.** Unless otherwise provided, when "written," "writing" and words of similar meaning are used in the Terms, they refer to both paper and electronic forms such as e-mails, faxes, digital images and copies, electronic notices capable of being stored and printed, and similar electronic versions.

**11.7.** Unless otherwise agreed in writing, the Bank may make any currency conversion using exchange rates that are reasonable in the relevant market at the time and for the size and type of the transaction.

**11.8.** The Customer will provide to the Bank all documents and other information reasonably requested by it in relation to any Account or Service.

**11. Загальні положення**

**11.1.** Ні Клієнт ні Банк не можуть уступати чи передавати свої права або обов'язки відповідно до цих Умов без попередньої письмової згоди іншої сторони, у наданні якої не може бути необґрунтовано відмовлено чи надання якої буде необґрунтовано затримуватися, за умови, що Банк може зробити таку передачу прав філії чи афілійованої особи, якщо це в значній мірі не матиме негативного впливу на надання послуг Клієнтові. Банк повинен повідомити про будь-яку таку передачу прав.

**11.2.** Якщо будь-яке положення цих Умов є або стає незаконним, нечинним або таким, що не може бути виконане в примусовому порядку відповідно до будь-якого чинного законодавства, інші положення цих умов матимуть повну силу (як і таке положення відповідно до будь-якого іншого законодавства).

**11.3.** Відмова або затримка зі сторони Клієнта чи Банку при застосуванні будь-якого права чи засобу правового захисту відповідно до цих Умов не означатимуть відмову від такого права. Будь-яка відмова від будь-якого права стосується лише конкретного випадку.

**11.4.** Клієнт і Банк дають згоду на телефонний чи електронний моніторинг чи запис з метою забезпечення безпеки та якості послуг та погоджують те, що будь-яка сторона може пред'явити записи телефонних розмов, дані електронних чи комп'ютерних систем як докази для будь-яких проваджень, порушених у зв'язку з Умовами.

**11.5.** Письмове повідомлення буде вважатися чинним, (i) якщо воно доставлене за основною робочою адресою Клієнта, яка вказана у Формі активації клієнта, а письмове повідомлення Банку на адресу Банку, визначену в останній виписці за відповідним Рахунком чи (ii) якщо воно надіслане на іншу таку адресу, яку одна сторона може повідомити іншій стороні письмово, включаючи електронну адресу для електронних повідомлень. Повідомлення складаються англійською мовою, якщо не погоджено інше чи інше не вимагається локальним законодавством.

**11.6.** Якщо не зазначено інше, коли слова «написаний», «письмова форма» та слова зі схожим значенням використовуються в Умовах, вони стосуються паперового та електронного формату, а саме електронної пошти, факсу, цифрових зображень та копій, електронних повідомлень, які можна зберігати та друкувати, та подібних електронних версій.

**11.7.** Якщо інше не узгоджено письмово, Банк може конвертувати будь-яку валюту, користуючись обмінними курсами, які є прийнятними на відповідному ринку на цей час та відповідно до розміру і типу транзакції.

**11.8.** Клієнт повинен надати Банкові всі документи та іншу інформацію, що можуть бути обґрунтовано необхідними у зв'язку з обслуговуванням Рахунку чи наданням Послуг.

**11.9.** Each party represents and warrants to the other party that (i) it has obtained and is in compliance with all necessary and appropriate consents, approvals and authorizations for the purposes of its entry into and performance of the Terms, and (ii) its entry into and performance of the Terms will not violate any applicable law or regulation.

**12. Law; Jurisdiction; Immunity**

**12.1.** In relation to any Account or Service, the Terms are governed by the law of the country or territory in which that Account is held or Service is provided, unless, in relation to Services, otherwise provided in a Service Agreement.

**12.2.** In relation to any Account or Service, the courts of the country or territory in which that Account is held or Service is provided have exclusive jurisdiction to hear any dispute arising out of or in connection with the Terms, unless, in relation to Services, otherwise provided in a Service Agreement, and the Customer and the Bank irrevocably submit to the jurisdiction of such courts.

**12.3.** Each of the Customer and the Bank waives to the fullest extent it can all immunities, whether sovereign or otherwise, it may have, including, without limitation, immunity from legal proceedings, immunity from execution of any judgment and immunity in respect of any form of relief that may be granted against it.

**11.9.** Будь-яка сторона повідомляє і гарантує іншій стороні, що (i) вона отримала і дотримується усіх необхідних і відповідних погоджень, дозволів і уповноважень для укладання цих Умов та їх виконання, і (ii) укладання і виконання Умов не порушують жодне чинне законодавство чи норми права.

**12. Законодавство. Юрисдикція. Імунітет**

**12.1.** Щодо будь-якого Рахунку чи Послуг ці Умови регулюються законодавством тієї країни чи території, де обслуговується Рахунок чи надаються Послуги, якщо щодо Послуг інше не передбачено Угодою про послуги.

**12.2.** Щодо будь-якого Рахунку чи Послуг суди країни чи території, в якій обслуговується Рахунок чи надаються Послуги, мають виключну юрисдикцію розглядати будь-які спори, що виникають в результаті чи у зв'язку з Умовами, якщо щодо Послуг інше не передбачено Угодою про послуги, і Клієнт та Банк безумовно підпорядковуються юрисдикції таких судів.

**12.3.** Як Клієнт, так і Банк відмовляються в повній мірі, наскільки це можливо, від права на імунітет, суверенний або інший, який вони можуть мати, включаючи, серед іншого, імунітет від судових проваджень, імунітет від виконання судового рішення та імунітет стосовно будь-якого засобу правового захисту, що може бути застосований проти них.

# CONFIDENTIALITY AND DATA PRIVAY CONDITIONS
# УМОВИ ПРО КОНФІДЕНЦІЙНІСТЬ ТА СЕКРЕТНІСТЬ ДАНИХ

**1. Introduction.**
These Conditions form part of the terms and conditions that apply between the Customer and the Bank in relation to the provision of Accounts and Services to the Customer. For the purpose of these Conditions, "Services" shall also include any services, transactions or dealings between the Bank and the Customer, whether or not related to the Customer's Account; these Conditions shall be in addition to any other terms and conditions agreed to between the Bank and the Customer. These Conditions set out each party's obligations in relation to Confidential Information and Personal Data received from the other party in connection with the provision of Accounts and Services. Some provisions of these Conditions are region-specific and will only apply in respect of the regions or countries specified. In some countries, further country- specific terms are required, and these will be included in the Local Conditions and/or Regulatory Disclosures, Declarations and Representations (RDDR) for that country. Except to the extent prohibited under applicable law or expressly agreed otherwise by the parties, and subject to any mandatory minimum notice period prescribed by applicable law, these Conditions may be updated from time to time with general applicability to customers upon written notice to the Customer. If there is a conflict between these Conditions and any agreement between the Bank and the Customer related to any Bank product or Service, the agreement related to the Bank product or Service prevails to the extent of any such conflict.

**1. Вступ.**
Ці Умови формують частину умов, які застосовуються Клієнтом та Банком стосовно обслуговування Рахунків чи надання Послуг Клієнтові. Для цілей цих Умов – поняття "Послуги" також включає будь-які послуги, трансакції або операції між Банком та Клієнтом, незалежно від того, чи пов'язані вони з Рахунком Клієнта; ці Умови можуть бути доповнені будь-якими іншими умовами, погодженими між Банком та Клієнтом. Ці Умови встановлюють обов'язки кожної сторони щодо збереження Конфіденційної інформації та Персональних даних, отриманих від іншої сторони у зв'язку із обслуговуванням Рахунків та наданням Послуг. Деякі положення цих Умов характерні для певного регіону і будуть застосовуватися тільки стосовно зазначених регіонів чи країн. В деяких країнах вимагаються спеціальні умови, що стосуються країни, і вони будуть включені в Місцеві умови для такої країни та/або в Законодавчі розкриття, Декларації та Твердження (RDDR) в цій країні. За винятком випадків, коли це заборонено згідно з чинним законодавством або якщо інше погоджено сторонами, та з урахуванням будь-якого обов'язкового мінімального строку повідомлення, встановленого чинним законодавством, ці Умови можуть оновлюватися час від часу та застосовуватимуться до клієнтів в загальному порядку і з письмовим повідомлення Клієнта. У разі виникнення протиріч між цими Умовами та будь-яким договором, укладеним між Банком та Клієнтом, що пов'язаний з будь-яким продуктом або Послугою Банку, договір, пов'язаний з продуктом або Послугою, матиме переважну сулу в разі виникнення будь-якого такого протиріччя.

**2. Protection of Confidential Information.**
The Receiving Party will keep the Disclosing Party's Confidential Information confidential on the terms hereof and exercise at least the same degree of care with respect to the Disclosing Party's Confidential Information that the Receiving Party exercises to protect its own Confidential Information of a similar nature, and in any event, no less than reasonable care.

**2. Захист Конфіденційної інформації.**
Одержуюча Сторона зберігатиме Конфіденційну інформацію Розкриваючої Сторони конфіденційною відповідно до цих правил і застосовуватиме принаймні той самий рівень захисту стосовно Конфіденційної інформації Розкриваючої Сторони, який Одержуюча Сторона застосовує для захисту власної Конфіденційної інформації аналогічного характеру, і, у будь-якому випадку, з не меншою розумною обережністю.

**3. Use and disclosure of Confidential Information.**
The Disclosing Party hereby grants the Receiving Party the right to use and disclose the Disclosing Party's Confidential Information to the extent necessary to accomplish the relevant Permitted Purposes. The Receiving Party will only use and disclose the Disclosing Party's Confidential Information to the extent permitted in these Conditions.

**3. Використання та розкриття Конфіденційної інформації.**
Розкриваюча Сторона цим надає право Одержуючій Стороні використовувати та розкривати Конфіденційну інформацію Розкриваючої Сторони тією мірою, що є необхідною для виконання відповідних Дозволених цілей. Одержуюча Сторона використовуватиме та розкриватиме Конфіденційну інформацію Розкриваючої Сторони, лише в межах дозволених цими Умовами.

**4. Exceptions to confidentiality.**
Notwithstanding anything in these Conditions to the contrary, the restrictions on the use and disclosure of Confidential Information in these Conditions do not apply to: information that: (i) is in or enters the public domain other than as a result of the wrongful act or omission of the Receiving Party or its Affiliates; or their respective Representatives in

**4. Винятки**
Незважаючи на будь-які положення цих Умов про протилежне, обмеження на використання та розкриття Конфіденційної інформації не застосовуються до: інформації, що: (i) є або стає публічною не в результаті протиправної дії чи бездіяльності Одержуючої Сторони або її Афілійованих осіб чи їх уповноважених

breach of these Conditions; (ii) is lawfully obtained by the Receiving Party from a third party or already known by the Receiving Party in each case without notice of any obligation to maintain it as confidential; (iii) was independently developed by the Receiving Party without reference to the Disclosing Party's Confidential Information; (iv) an authorized officer of the Disclosing Party has agreed in writing that the Receiving Party may disclose on a non-confidential basis; or (v) constitutes Anonymized and/or Aggregated Data.

Представників стосовно порушення цих Умов; (ii) є законно отриманою Одержуючою Стороною від третьої сторони чи вже є відомою Одержуючій Стороні у будь-якому випадку без повідомлення про будь-яке зобов'язання зберігати її конфіденційність; (iii) була незалежно розробленою Одержуючою Стороною без посилання на Конфіденційну інформацію Розкриваючої Сторони; (iv) було письмово погоджено уповноваженою службовою особою Розкриваючої Сторони, що Одержуюча Сторона може розкрити таку інформацію на неконфіденційній основі; чи (v) становить Анонімні та/або Збірні дані.

**5. Authorized disclosures.**

**5.1 Affiliates and Representatives.**

Receiving Party may disclose the Disclosing Party's Confidential Information to the Receiving Party's Affiliates and to those of the Receiving Party's and its Affiliates' respective Representatives who have a "need to know" such Confidential Information, although only to the extent necessary to fulfil the relevant Permitted Purposes. The Receiving Party shall ensure that any of its Affiliates and Representatives to whom the Disclosing Party's Confidential Information is disclosed pursuant to this Condition 5.1 shall be bound to keep such Confidential Information confidential and to use it for only the relevant Permitted Purposes.

**5. Уповноважене розкриття.**

**5.1 Афілійовані особи та Представники.**

Одержуюча Сторона може розкрити Конфіденційну інформацію Розкриваючої Сторони Афілійованим особам Одержуючої Сторони, та уповноваженим Представникам Одержуючої Сторони, у яких є «потреба знати» таку Конфіденційну інформацію, однак тільки в обсягах, необхідних для виконання Дозволених цілей. Одержуюча Сторона гарантує забезпечити, що будь-хто з її Афілійованих осіб та Представників, яким Конфіденційна інформація Розкриваючої Сторони розкрита відповідно до цього пункту 5.1 будуть зобов'язані забезпечувати її конфіденційність та використовувати її лише для відповідних Дозволених цілей.

**5.2 Other disclosures.**

With respect to the Customer's Confidential Information, Bank Recipients may: (i) disclose it to such third parties as may be designated by the Customer (for example, the Customer's shared service center) and to Customer Affiliates; (ii) disclose it to Payment Infrastructure Providers on a confidential basis to the extent necessary for the operation of the Account and the provision of the Services; and (iii) use it and disclose it to other Bank Recipients for the purpose of supporting the opening of accounts by, and the provision of Services to, the Customer and Customer Affiliates at and by the Bank and Bank Affiliates.

**5.2 Інші випадки розкриття Конфіденційної інформації.**

Що стосується Конфіденційної інформації Клієнта, то Одержувачі Банку можуть: (i) розкрити її тим третім сторонам, яких визначає Клієнт (наприклад, Спільному центру послуг Клієнта), та Афілійованим особам Клієнта; (ii) розкривати ii Постачальникам платіжної інфраструктури на конфіденційній основі в межах, необхідних для виконання операцій з обслуговування Рахунку та надання Послуг; (iii) використовувати та розкривати її іншим Одержувачам Банку, отриману від Клієнта з метою відкриття рахунків Клієнтом та Афілійованими особами Клієнта і надання їм Послуг у Банку та Банком, а також у Афілійованим особам Банку та Афілійованими особами Банку.

**5.3 Payment reconciliation.**

When the Customer instructs the Bank to make a payment from an Account to a third party's account, in order to enable the third party to perform payment reconciliations, the Bank may disclose to the third party the Customer's name, address and account number (and such other Customer Confidential Information as may be reasonably required by the third party to perform payment reconciliations).

**5.3 Погодження платежу.**

Коли Клієнт надає інструкції Банку здійснити платіж зі свого Рахунку на рахунок третьої сторони, для здійснення перевірки платежу третьою стороною, Банк може розкрити третій стороні найменування Клієнта, адресу і номер рахунку (та іншу Конфіденційну інформацію Клієнта, яка може належним чином вимагатися третьою стороною, щоб здійснити узгодження платежу).

**5.4 Legal and regulatory disclosure.**

The Receiving Party (and, where the Bank is the Receiving Party, Bank Recipients and Payment Infrastructure Providers) may disclose the Disclosing Party's Confidential Information pursuant to legal process, or pursuant to any other foreign or domestic legal and/or regulatory obligation or request, or agreement entered into by any of them and any governmental authority, domestic or foreign, or between or among any two or more domestic or foreign governmental authorities, including disclosure to courts, tribunals, and/or legal, regulatory, tax and government authorities.

**5.4 Юридичне та нормативне розкриття.**

Одержуюча Сторона (і у випадках, коли Банк є Одержуючою Стороною Одержувачі банку та Постачальники платіжної інфраструктури) може розкрити Конфіденційну інформацію, якщо це вимагається відповідно до судового процесу або відповідно до будь-якого іншого іноземного або внутрішньодержавного юридичного та/або нормативного зобов'язання чи вимоги, або угоди, укладеної між будь-ким з них і будь-яким державним органом влади, внутрішньодержавним чи іноземним, або між будь-якими двома або більше внутрішньодержавними або іноземними органами влади, включаючи розкриття судам, трибуналам та/або юридичним, регулюючим, податковим та державним органам влади.

**6. Retention and deletion.**

**6. Право на збереження та знищення.**

On closure of Accounts, termination of the provision of the Services, each of the Customer and Bank Recipients shall be entitled to retain and use the other party's Confidential Information, subject to the confidentiality and security obligations herein, for legal, regulatory, audit and internal compliance purposes and in accordance with their internal records management policies to the extent that this is permissible under applicable laws and regulations, but shall otherwise securely destroy or delete such Confidential Information.

При закритті Рахунків, припиненні надання Послуг кожному Клієнтові та усім Одержувачам Банку надається право зберігати та використовувати Конфіденційну інформацію іншої сторони, виконуючи при цьому зобов'язання щодо забезпечення конфіденційності або безпеки, передбачені цими Умовами, дотримуючись законних, нормативних, аудиторських цілей, внутрішніх цілей, а також дотримуючись внутрішньої політики управління документообігом в межах дозволених чинним законодавством, однак в іншому випадку Конфіденційну інформацію слід знищити або видалити.

**7. Data privacy.**

**7.1 Compliance with law.**

The Receiving Party will comply with applicable Data Protection Law in Processing Disclosing Party Personal Data in connection with the provision or receipt of Accounts and Services.

**7. Захист даних.**

**7.1 Дотримання законодавства.**

Одержуюча Сторона повинна дотримуватися чинного Законодавства Щодо Захисту Даних при Обробці персональних даних Розкриваючої Сторони у зв'язку з обслуговуванням Рахунку та наданням або отриманням Послуг.

**7.2 Compliance with GDPR/Equivalent Laws.**

Without limiting Condition 7.1 (Compliance with law), to the extent that the Processing of Personal Data is subject to the GDPR or any Equivalent Law: (i) each party is responsible for its own compliance with applicable Data Protection Law; and (ii) the Customer confirms that any Customer Personal Data that it provides to the Bank has been Processed fairly and lawfully, is accurate and is relevant for the purposes for which it is being provided and the Bank may rely on the Customer's compliance with such undertaking and, where applicable, assistance from the Customer pursuant to Condition 7.6 (Legal basis for Processing).

**7.2 Дотримання ЗРЗД/Еквівалентного законодавства.**

Не обмежуючи умову 7.1 (Дотримання законодавства), оскільки Обробка персональних даних підпадає під дію ЗРЗД або будь-якого Еквівалентного законодавства: (i) кожна сторона несе відповідальність за власне дотримання діючого Законодавства Щодо Захисту Даних; і (ii) Клієнт підтверджує, що будь-які Персональні дані Клієнта, які він надає Банку, були оброблені чесно та законно, є точними та актуальними для цілей, для яких вони надані, і Банк може покладатися на дотримання Клієнтом вимог законодавства та, де це може бути застосовано, на допомогу Клієнта відповідно до умов 7.6 (Правова база для Обробки).

**7.3 Security.**

The Bank will, and will use reasonable endeavors to ensure that Bank Affiliates and Third Party Service Providers will, implement reasonable and appropriate technical and organizational security measures to protect Customer Personal Data that is within its or their custody or control against unauthorized or unlawful Processing and accidental destruction or loss.

**7.3 Безпека.**

Банк забезпечуватиме і вживатиме відповідних заходів щоб Афілійовані особи та Інші постачальники послуг забезпечували встановлення розумних і належних технічних та організаційних заходів безпеки для захисту Персональних даних Клієнта які знаходяться в його розпорядженні або під його контролем, від несанкціонованої або незаконної Обробки та випадкового знищення чи втрати.

**7.4 Purpose limitation.**

The Customer hereby authorizes the Bank to Process Customer Personal Data in accordance with these Conditions and to the extent reasonably required for the relevant Permitted Purposes for the period of time reasonably necessary for the relevant Permitted Purposes.

**7.4 Обмеження.**

Цим Клієнт уповноважує Банк обробляти Персональні дані Клієнта відповідно до цих Умов та до тієї міри, що належним чином вимагається для відповідних Дозволених цілей на період часу, що є обґрунтовано необхідним для відповідних Дозволених цілей.

**7.5 International transfer.**

The Customer acknowledges that in the course of the disclosures described in Condition 5 (Authorized disclosures), Disclosing Party Personal Data may be disclosed to recipients located in countries which do not offer a level of protection for those data as high as the level of protection in the country in which the Bank is established or the Customer is located.

**7.5 Міжнародна передача.**

Клієнт підтверджує, що в процесі розкриття, зазначеного в статті 5 (Уповноважене розкриття), Персональні дані Розкриваючої Сторони можуть бути розкриті одержувачам, які знаходяться в країнах, що не надають такий самий високий рівень захисту для цих даних, який існує в країні, де знаходиться Банк або Клієнт.

**7.6 Legal basis for Processing.**

**7.6.1** Except as noted in Condition 7.6.2:

**(A) When the Customer is the Data Subject**: To the extent that the Customer is the Data Subject of Customer Personal Data Processed by the Bank, then the Customer consents to the Bank's Processing of all of such Customer Personal Data as described in Conditions 3 to 7.

**7.6 Юридичне підґрунтя для Обробки.**

**7.6.1** За винятками, переліченими в Умові 7.6.2:

**(A) Коли Клієнт є Суб'єктом Персональних даних:** До того часу, поки Клієнт є Суб'єктом Персональних даних Клієнта, що Обробляються Банком, Клієнт погоджується на обробку Банком усіх таких Персональних даних Клієнта, як це передбачено в статтях 3-7.

**(B) When the Customer is not the Data Subject**: to the extent that the Bank Processes Customer Personal Data about other Data Subjects (for example, the Customer's personnel or Related Parties), the Customer warrants that to the extent required by applicable law or regulation, it has provided notice to and obtained consent from such Data Subjects in relation to the Bank's Processing of their Personal Data as described in these Conditions (and will provide such notice or obtain such consent in advance of providing similar information in future). The Customer further warrants that any such consent has been granted by these Data Subjects for the period reasonably required for the realization of the relevant Permitted Purposes.

**7.6.2** To the extent that the Processing of Personal Data is subject to the GDPR or any Equivalent Law then the provisions of this Condition 7.6.2 shall apply:

**(A) When the Customer is the Data Subject:** when the Customer is the Data Subject of Customer Personal Data Processed by the Bank, then the Customer hereby acknowledges that the Bank will Process Customer Personal Data as set forth in the relevant TTS Privacy Statement accessible at https://www.citibank.com/tts/sa/tts-privacy-statements/index.html (or such other URL or statement as the Bank may notify to the Customer from time to time) and the Bank may seek consent prior to conducting certain Processing activities from the Customer from time to time as its legal basis for Processing Customer Personal Data under the GDPR or any Equivalent Law; and

**(B) When the Customer is not the Data Subject**: when the Bank Processes Customer Personal Data about other Data Subjects (for example, the Customer's personnel or Related Parties), the Customer warrants that it shall provide notice to, and shall seek consent from (and promptly upon the Bank's request shall provide evidence to the Bank of having provided such notices and/or obtained such consents) such Data Subjects in relation to the Bank's Processing of their Personal Data in accordance with any instructions of the Bank from time to time (which may include the form and the manner in which a notice is to be provided, or any consent is to be obtained). In connection with the foregoing, the Customer warrants that it will provide Data Subjects with a copy of the relevant TTS Privacy Statement accessible at https://www.citibank.com/tts/sa/tts-privacy-statements/index.html (or such other URL or statement as the Bank may notify to the Customer from time to time).

**7.7 Employee reliability and training.**
The Bank will take reasonable steps to ensure the reliability of its employees who will have access to Customer Personal Data and will ensure that those of its employees who are involved in the Processing of Customer Personal Data have undergone appropriate training in the care, protection and handling of Personal Data.

**7.8 Audit.**
The Bank shall provide the Customer with such information as is reasonably requested by the Customer to enable the Customer to satisfy itself of the Bank's compliance with its obligations under Condition 7.3 (Security). Nothing in this Condition 7.8 shall have the effect of requiring the Bank to provide information that may cause it to breach its confidentiality obligations to third parties.

**(В) Коли Клієнт не є Суб'єктом Персональних даних**: До того часу поки Банк Обробляє Персональні дані Клієнта про інших Суб'єктів даних (наприклад, персонал Клієнта чи Пов'язаних сторін), Клієнт гарантує, що в межах, необхідних відповідно до чинного законодавства, Клієнт повідомив та отримав згоду від Суб'єктів таких даних на Обробку Банком їхніх Персональних даних, згідно цих Умов (і заздалегідь надасть таке повідомлення або отримає таку згоду на надання подібної інформації у майбутньому). Клієнт гарантує, що будь-яка така згода надається цими Суб'єктами даних на період, що належним чином вимагається для реалізації відповідних Дозволених цілей.

**7.6.2** До того часу поки Обробка Персональних даних є предметом ЗРЗД чи будь-якого Еквівалентного законодавства, положення пункту 7.6.2. цих Умов мають застосовуватися:

**(А) Коли Клієнт є Суб'єктом Персональних даних**: коли Клієнт являється Суб'єктом даних Персональних даних Клієнта, що обробляються Банком, Клієнт цим підтверджує, що Банк буде обробляти Персональні дані Клієнта, як це встановлено у відповідній Заяві про конфіденційність Казначейських та Комерційних рішень, доступній на https://www.citibank.com/tts/sa/tts-privacy-statements/index.html (або іншій URL-адресі або в іншій заяві про які Банк може час від часу інформувати Клієнта), і Банк може вимагати згоди від Клієнта до здійснення певних процесів обробки як юридичну основу для обробки Персональних даних Клієнта як це вимагається ЗРЗД або будь-яким Еквівалентним законодавством і

**(В) коли Клієнт не являється Суб'єктом даних**: до того часу поки Банк Обробляє Персональні дані Клієнта про інших Суб'єктів даних (наприклад, персонал Клієнта чи Пов'язаних сторін), Клієнт гарантує, що він проінформує та отримає згоду (і негайно на вимогу Банку надасть докази Банку про надання таких повідомлень та / або отримання таких згод) від таких Суб'єктів даних по відношенню до обробки їхніх Персональних даних Банком у відповідності з інструкціями Банку, що надаватимуться час від часу (які можуть включати форму та спосіб у якій повідомлення має бути надане). У зв'язку з вищезазначеним Клієнт гарантує, що надасть Суб'єкту даних копію відповідного Положення про конфіденційність Казначейських та Комерційних рішень, доступному на https://www.citibank.com/tts/sa/tts-privacy-statements/index.html (або іншій URL-адресі або виписці, про що Банк може інформувати Клієнта періодично).

**7.7 Надійність та навчання працівників.**
Банк повинен вживати належних заходів, щоб забезпечити надійність своїх працівників, які мають доступ до Персональних даних Клієнта, і повинен забезпечити, що працівники, які займаються обробкою Персональних даних Клієнта, пройшли відповідне навчання з обробки, захисту та поводження з Персональними даними.

**7.8 Аудит.**
Банк повинен надати Клієнту інформацію, яка обґрунтовано вимагається Клієнтом, щоб переконатися в дотриманні Банком його зобов'язань відповідно до пункту 7.3 (Конфіденційність та безпека). Ніщо в пункті 7.8 не повинно вважатися підставою для того, щоб вимагати від Банку надання інформації, що може спричинити

**8. Security Incidents.**
If the Bank becomes aware of a Security Incident, the Bank will investigate and remediate the effects of the Security Incident in accordance with its internal policies and procedures and the requirements of applicable law and regulation. The Bank will notify the Customer of any Security Incident as soon as reasonably practicable after the Bank becomes aware of a Security Incident, unless the Bank is subject to a legal or regulatory constraint, or if it would compromise the Bank's investigation. The parties agree that in relation to a Security Incident, each party will be responsible for making any notifications to regulators and individuals that are required under applicable Data Protection Law. Each party will provide reasonable information and assistance to the other party to the extent necessary to help the other party to meet its obligations to Data Subjects and regulators. Neither the Bank nor the Customer will issue press or media statements or comments in connection with the Security Incident that name the other party unless it has obtained the other party's prior written consent.

**9. Definitions**
Capitalised terms used in these Conditions shall have the meanings given to them in the Master Account and Service Terms or as set out below:

**"Affiliate"** means either a Bank Affiliate or a Customer Affiliate, as the context may require;

**"Anonymized and/or Aggregated Data"** means information relating to the Disclosing Party received or generated by the Receiving Party in connection with the provision or receipt of the Account and Services and in respect of which all direct personal identifiers have been removed, and/or which has been aggregated with other data, in both cases such that the data cannot reasonably identify the Disclosing Party, its Affiliates or a natural person;

**"Bank Affiliate"** means any entity, present or future, that directly or indirectly Controls, is Controlled by or is under common Control with the Bank, and any branch or representative offices thereof, including Citibank, N.A. and Citigroup Technologies, Inc.;

**"Bank Personal Data"** means Personal Data relating to a Data Subject received by the Customer from the Bank, Bank Affiliates and/or their respective Representatives in the course of receiving Accounts and Services from the Bank. Bank Personal Data may include names and contact details, to the extent that these amount to Personal Data under applicable Data Protection Law;

**"Bank Recipients"** means the Bank, Bank Affiliates and their respective Representatives;

**"Conditions"** means these Confidentiality and Data Privacy Conditions;

**"Confidential Information"** means:

порушення ним зобов'язань про конфіденційність перед третіми сторонами.

**8. Інциденти інформаційної безпеки.**
Якщо Банку стає відомо про будь-який Інцидент інформаційної безпеки, Банк повинен провести розслідування та усунути наслідки такого Інциденту інформаційної безпеки відповідно до внутрішніх політики та процедур і вимог чинного законодавства. Банк повинен повідомити Клієнта про будь-який Інцидент інформаційної безпеки у найкоротші, обґрунтовано можливі строки після того, як Банку стане відомо про Інцидент інформаційної безпеки, за умови, що Банк не підлягає законодавчому обмеженню і це не поставить розслідування Банку під загрозу. Сторони погоджуються, що по відношенню доІнциденту інформаційної безпеки, кожна сторона буде зобов'язана повідомляти регулюючим органам та фізичним особам, якщо це вимагається відповідно до чинного законодавства про захист даних. Кожна сторона повинна надавати належну інформацію та допомогу іншій стороні в тій мірі, в якій це необхідно, щоб кожна сторона змогла виконати свої обов'язки перед Суб'єктами даних та регулюючими органами. Ні Банк, ні Клієнт не повинні робити заяви чи давати коментарі в пресі та медіа стосовно Інциденту інформаційної безпеки, де згадується інша сторона, якщо на це не отримано письмову згоду іншої сторони.

**9. Визначення.**
Терміни, написані з великої букви в цих Умовах, мають значення, дані їм в Генеральних умовах обслуговування рахунку та надання послуг, або відповідно до визначень нижче:

**«Афілійована особа»** означає або Афілійовану особу Банку, або Афілійовану особу Клієнта, відповідно до контексту;

**«Анонімні та/або збірні дані»** означають інформацію Розкриваючої Сторони , що була одержана чи вироблена Одержуючою Стороною, у зв'язку з обслуговуванням Рахунку та надання Послуг та щодо якої усі прямі Персональні ідентифікатори були видалені, та/або були зібрані з іншими даними; в обох випадках такі дані не можуть достатньо ідентифікувати Розкриваючу Сторону, її Афілійованих осіб або фізичну особу;

**«Афілійована особа Банку»** означає будь-яку організацію, яка існує зараз або буде існувати у майбутньому, яка прямо або опосередковано Контролює, Контролюється або знаходиться під загальним Контролем Банку, а також будь-яке її відділення або представництво, включаючи Citibank, N.A. та Citigroup Technologies, Inc.;

**«Персональні дані Банку»** означають Персональні дані, пов'язані з Суб'єктом даних, отримані Клієнтом від Банку, Афілійованих осіб Банку та/або їхніх відповідних Представників в процесі обслуговування Рахунку та надання Послуг. Персональні дані Банку можуть включати імена та контакти, якщо вони становлять Персональні дані відповідно до Законодавства щодо захисту даних;

**«Одержувачі Банку»** означають Банк, Афілійовані особи Банку та їхніх відповідних Представників;

**«Умови»** означають ці Умови про конфіденційність та секретність даних;
**«Конфіденційна інформація» означає:**

(A) where the Disclosing Party is the Customer or a Customer Affiliate, or any of their respective Representatives: information relating to the Customer or Customer Affiliates or their respective Representatives or Related Parties received by Bank Recipients in the course of providing Accounts and Services to the Customer, including all Customer Personal Data, Customer's bank account details, transactional information, and any other information which is either designated by the Customer as confidential at the time of disclosure or that a reasonable person would consider to be of a confidential or proprietary nature; or

(A) там, де Розкриваючою Стороною є Клієнт, Афілійована особа Клієнта чи будь-який відповідний Представник: інформація Клієнта, Афілійованих осіб Клієнта, їх відповідних Представників чи Пов'язаних сторін, отриману Одержувачами Банку в процесі обслуговування Рахунку чи надання Послуг, включаючи усі Персональні дані Клієнта, дані банківського рахунку Клієнта, інформацію щодо операції і будь-яку іншу інформацію, яка або визначена Клієнтом як конфіденційна на момент розкриття, або яку відповідна особа визначила б як інформацію конфіденційного або приватного характеру; або

(B) where the Disclosing Party is the Bank or a Bank Affiliate, or any of their respective Representatives: information relating to the Bank or Bank Affiliates or their respective Representatives received or accessed by the Customer, Customer Affiliates and their respective Representatives in connection with the receipt of Accounts and Services from the Bank, including Bank Personal Data, information relating to the Bank's products and services and the terms and conditions on which they are provided, technology (including software, the form and format of reports and online computer screens), pricing information, internal policies, operational procedures and any other information which is either designated by the Bank as confidential at the time of disclosure or that a reasonable person would consider to be of a confidential or proprietary nature;

(B) там, де Розкриваючою Стороною є Банк, Афілійована особа Банку або будь-який відповідний Представник: інформація Банку, Афілійованих осіб Банку, їхніх відповідних Представників отриману Клієнтом, Афілійованими особами Клієнта та їхніми відповідними Представниками в процесі обслуговування Рахунків чи надання Послуг, включаючи Персональні дані Банку, інформацію, пов'язану з продукцією, послугами та умовами, на яких вони надаються, технології (зокрема програмні засоби, форми і формати звітів та інтерактивні комп'ютерні дані), інформацію про ціни, внутрішні політики, процедури щодо операцій та будь-яку іншу інформацію, яка або визначена Банком як конфіденційна на момент розкриття, або яку відповідна особа визначила б як інформацію конфіденційного або приватного характеру;

**"Control"** means that an entity possesses directly or indirectly the power to direct or cause the direction of the management and policies of the other entity, whether through the ownership of voting shares, by contract or otherwise;

**«Контроль»** означає те, що організація має пряме або опосередковане право управляти або забезпечувати керування менеджментом та політикою іншої організації внаслідок володіння акціями з правом голосу, на підставі договору або в інший спосіб;

**"Customer Affiliate"** means any entity, present or future, that directly or indirectly Controls, is Controlled by, or is under common Control with the Customer, and any branch thereof;

**«Афілійована особа Клієнта»** означає будь-яку організацію, яка існує зараз або буде існувати у майбутньому, яка прямо або опосередковано Контролює, Контролюється або знаходиться під загальним Контролем Клієнта, а також будь-яке її відділення;

**"Customer Personal Data"** means Personal Data relating to a Data Subject received by or on behalf of the Bank from the Customer, Customer Affiliates and their respective Representatives and Related Parties in the course of providing Accounts and Services to the Customer. Customer Personal Data may include names, contact details, identification and verification information, nationality and residency information, taxpayer identification numbers, voiceprints, bank account and transactional information (where legally permissible), to the extent that these amount to Personal Data under applicable Data Protection Law;

**«Персональні дані Клієнта»** означають Персональні дані, пов'язані з Суб'єктом даних, отримані Банком або від імені Банку від Клієнта, Афілійованих осіб Клієнта та їхніх відповідних Представників та Пов'язаних сторін в процесі обслуговування Рахунків або надання Послуг Клієнту. Персональні дані Клієнта можуть включати імена, контактну інформацію, ідентифікаційні дані, дані про результати перевірки, інформацію про громадянство та місце проживання, ідентифікаційні номери платників податків, голосові позначки, інформацію про банківський рахунок та операції за ним (де це дозволено законом), в тій мірі, наскільки вони можуть вважатися Персональними даними відповідно до чинного локального законодавства щодо захисту або конфіденційності даних;

**"Data Protection Law"** means any and all applicable laws and/or regulations relating to privacy and/or data protection in relation to the Processing of Customer Personal Data or Bank Personal Data, including any amendments or supplements to or replacements of such laws and/or regulations and including without limitation and as applicable: (i) the EU Directive on Data Protection (95/46/EC) and the EU Directive on Privacy and Electronic Communications (2002/58/EC); (ii) any national laws implementing such directives; (iii) the "GDPR"; and (iv) any Equivalent Law;

**«Законодавство щодо захисту даних»** означає будь-які та всі застосовні закони та/чи нормативно-правові акти, що стосуються обробки Персональних даних Клієнта чи Персональних даних Банку, включаючи будь-які зміни, поправки чи доповнення до таких законів чи нормативно-правових актів, включаючи, але не обмежуючись, якщо це може бути застосовано: (i) Директива Європейського комітету з захисту даних (95/46 / ЄС) та Директива про конфіденційність та електронні засоби зв'язку (2002/58 / ЄС); (ii) будь-які національні закони, які запроваджують такі директиви; (iii) Загальний Регламент Захисту Даних (ЗРЗД) і (iv) Еквівалентне законодавство;

| | |
|---|---|
| **"Data Subject"** means a natural person who is identified, or who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity, or, if different, the meaning given to this term or nearest equivalent term under applicable Data Protection Law. For the purpose of these Conditions, Data Subjects may be the Customer, Customer Affiliates, the Bank, their personnel, Related Parties, customers, suppliers, payment remitters, payment beneficiaries or other persons; | «Суб'єкт даних» означає фізичну особу, ідентифіковану, або таку, що може бути ідентифікованою прямо або опосередковано, з посиланням на такі ідентифікатори як ім'я, ідентифікаційний номер, інформацію про місцезнаходження, онлайн ідентифікатори або на одну або кілька ознак фізичної, фізіологічної, психічної, генетичної, економічної, культурної та соціальної приналежності, або, у інших випадках, відповідно до чинного Законодавства щодо захисту даних. У контексті цих Умов Суб'єктами даних можуть бути Клієнт, Афілійовані особи Клієнта, Банк, їх персонал, Пов'язані сторони, клієнти, постачальники, відправники грошового переказу, отримувачі грошового переказу або інші особи; |
| **"Disclosing Party"** means a party that discloses Confidential Information to the other party; | **«Розкриваюча Сторона»** означає сторону, що розкриває Конфіденційну інформацію іншій стороні; |
| **"Disclosing Party Personal Data"** means Customer Personal Data or Bank Personal Data, as the context permits; | **«Персональні дані Розкриваючої Сторони»** означають Персональні дані Клієнта чи Персональні дані Банку, відповідно до контексту; |
| **"Equivalent Law"** means the laws and/or regulations of any country outside the EEA that are intended to provide equivalent protections for Personal Data (or the nearest equivalent term under applicable data protection law and/or regulation) of Data Subjects as the GDPR, including without limitation, the data protection laws of Jersey, Macau, Morocco, Switzerland and the United Kingdom; | **«Еквівалентне законодавство»** означає закони і положення будь-якої країни за межами Європейського союзу, які призначені для забезпечення еквівалентного захисту Персональних даних (або найближчого еквівалентного терміну відповідно до чинного законодавства та / або нормативних актів що регулюють захист персональних даних) Суб'єктів даних, таких як ЗРЗД, включаючи, але не обмежуючись, закони про захист персональних даних Джерсі, Макао, Марокко, Швейцарії та Сполученого Королівства; |
| "**GDPR**" means the General Data Protection Regulation (EU) 2016/679 and any laws and/or regulations implementing or made pursuant to such regulation; | **«ЗРЗД»** означає Загальний Регламент Захисту Даних (ЄС) та будь-які закони чи інші нормативні акти, що запроваджують регламент чи постановляються відповідно до такого регламенту. |
| **"Payment Infrastructure Provider"** means a third party which forms part of a payment system infrastructure, including without limitation communications, clearing or payment systems, intermediary banks and correspondent banks; | **«Постачальник платіжної інфраструктури»** означає третю сторону, яка формує частину інфраструктури платіжної системи, включаючи, серед іншого, комунікації, клірингові чи платіжні системи, банки-посередники або банки-кореспонденти; |
| **"Permitted Purposes"** in relation to the Bank's use of the Customer's Confidential Information means the following purposes: (A) to provide Accounts and Services to the Customer in accordance with the Terms; (B) to undertake activities related to the provision of Accounts and Services, such as, by way of non-exhaustive example: (1) to fulfil foreign and domestic legal, regulatory and compliance requirements (including US anti-money laundering obligations applicable to the Bank's parent companies) and comply with any applicable treaty or agreement with or between foreign and domestic governments applicable to any of the Bank, Bank Affiliates and their agents or Payment Infrastructure Providers; (2) to verify the identity of Customer representatives who contact the Bank or may be contacted by the Bank; (3) for risk assessment, information security management, statistical, trend analysis and planning purposes; (4) to monitor and record calls and electronic communications with the Customer for quality, training, investigation and fraud prevention purposes; (5) for crime detection, prevention, investigation and prosecution; (6) to enforce or defend the Bank's or Bank Affiliates' rights; and (7) to manage the Bank's relationship with the Customer, which may include providing information to Customer and Customer Affiliates about the Bank's and Bank Affiliates' products and services; (C) the purposes set out in Condition 5 (Authorized disclosures); (D) any additional purposes expressly authorised by the Customer; and (E) any additional purposes as may be notified to the Customer or Data Subjects in any notice provided by, or upon the instruction of, the Bank pursuant to Condition 7.6.2 ; | **«Дозволені цілі»** у контексті використання Банком Конфіденційної інформації Клієнта означають наступні цілі: (А) обслуговувати Рахунки та надавати Послуги Клієнту відповідно до Умов; (Б) виконувати діяльність, пов'язану з обслуговуванням Рахунків чи наданням Послуг, як наведено у наступному неповному прикладі: (1) дотримуватися іноземних та вітчизняних законодавчих вимог та внутрішніх норм (включаючи норми США про зобов'язання про боротьбу з відмиванням грошей, що застосовуються до головних компаній Банку) та дотримуватися будь-якого чинного договору або угоди з іноземними та внутрішніми органами влади або між ними, дія якої поширюється на будь-який Банк, Афілійовані особи Банку та їхніх агентів чи Постачальників платіжної інфраструктури; (2) перевіряти особу представників Клієнта, які контактують з Банком або з якими може контактувати Банк; (3) оцінювати ризики, здійснювати менеджмент безпеки інформації, статистичний аналіз та аналіз тенденцій і цілей планування; (4) здійснювати моніторинг і запис дзвінків та здійснювати електронне спілкування з Клієнтом з метою забезпечення якості надання послуг, проведення навчання, розслідування та попередження шахрайства; (5) виявляти, попереджати, розслідувати злочини; (6) підсилювати або захищати права Банку або афілійованих осіб Банку; та (7) управляти відносинами Банку та Клієнта, які можуть включати надання інформації Клієнту та Афілійованим особам Клієнта про продукцію і послуги Банку та Афілійованих осіб Банку; (В) дотримуватися цілей, визначених в статті 5 (Уповноважене розкриття); (Г) будь-які інші |

| | |
|---|---|
| | цілі, чітко визначені Клієнтом; та (ґ) будь-які інші додаткові цілі, про які може бути повідомлено Клієнту чи Суб'єктам даних у будь-якому повідомленні, наданому Банком або відповідно до інструкцій Банку, відповідно до умов 7.6.2; |
| **"Permitted Purposes"** in relation to the Customer's use of the Bank's Confidential Information means the following purposes: to enjoy the benefit of, enforce or defend its rights and perform its obligations in connection with the receipt of Accounts and Services from the Bank in accordance with the Terms, and to manage the Customer's relationship with the Bank; | **«Дозволені цілі»** у контексті використання Клієнтом Конфіденційної інформації Банку означають наступні цілі: користуватися своїми правами, забезпечувати виконання чи захищати свої права та виконувати свої обов'язки у зв'язку з обслуговуванням Рахунку та надання Послуг Банком відповідно до Умов, а також управляти відносинами Клієнта з Банком; |
| **"Personal Data"** means any information that can be used, directly or indirectly, alone or in combination with other information, to identify a Data Subject, or if different, the meaning given to this term or nearest equivalent term under applicable Data Protection Law; | **«Персональні дані»** означають будь-яку інформацію, що може бути використана, прямо або опосередковано, самостійно або в комбінації з іншою інформацією для ідентифікації фізичної особи, або, у інших випадках, якщо інше визначення дане цьому термінові або найближчому відповідному термінові згідно з чинним Законодавством щодо захисту даних; |
| **"Processing"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, or, if different, the meaning given to this term or nearest equivalent term under applicable Data Protection Law; | **«Обробка»** означає будь-яку операцію або низку операцій, які виконуються з Персональними даними або низкою Персональних даних автоматичними або неавтоматичними засобами, наприклад, збирання, запис, організація, структурування, зберігання, адаптація або зміна, повернення, консультація, використання, розкриття через передачу, поширення або забезпечення доступу в інший спосіб, регулювання або поєднання, обмеження, стирання або знищення, або, якщо інше визначення дане цьому термінові чи найближчому відповідному термінові відповідно до чинного Законодавства щодо захисту даних; |
| **"Receiving Party"** means a party that receives Confidential Information from the other party; | **«Одержуюча Сторона,»** означає сторону, що отримує Конфіденційну інформацію від іншої сторони; |
| **"Related Party"** means any natural person or entity, or branch thereof, that: (i) owns, directly or indirectly, stock of the Customer, if the Customer is a corporation, (ii) owns, directly or indirectly, profits, interests or capital interests in the Customer, if the Customer is a partnership, (iii) is treated as the owner of the Customer, if the Customer is a "grantor trust" under sections 671 through 679 of the United States Internal Revenue Code or is of equivalent status under any similar law of any jurisdiction, domestic or foreign, (iv) holds, directly or indirectly, beneficial interests in the Customer, if the Customer is a trust; or (v) exercises control over the Customer directly or indirectly through ownership or any arrangement or other means, if the Customer is an entity, including: (a) a settlor, protector or beneficiary of a trust; (b) a person who ultimately has a controlling interest in the Customer; (c) a person who exercises control over the Customer through other means; or (d) the senior managing official of the Customer; | **«Пов'язана сторона»** означає будь-яку фізичну особу чи організацію, чи її відділення, що: (і) володіє, прямо або опосередковано, акціями Клієнта, якщо Клієнт є корпорацією, (іі) володіє, прямо або опосередковано, прибутками, відсотками чи частиною капіталу Клієнта, якщо Клієнт є товариством, (ііі) вважається власником Клієнта, якщо Клієнт є «трастом, який надає дотацію» відповідно до розділів 671-679 Внутрішнього податкового кодексу США чи має рівнозначний статус відповідно до будь-якого аналогічного закону будь-якої юрисдикції, внутрішньодержавної чи іноземної, (iv) володіє, прямо або опосередковано, бенефіціарними частками Клієнта, якщо Клієнт є трастом; або (v) здійснює контроль над Клієнтом, прямо або опосередковано, через володіння, будь-який договір або в інший спосіб, якщо Клієнт є організацією, зокрема: (а) особою, яка укладає акт розпорядження майном на користь іншої особи, захисником або бенефіціаріем трасту; (б) особою, яка, зрештою, має контрольний пакет в капіталі Клієнта; (в) особою, яка здійснює контроль над Клієнтом через інші засоби, або (г) посадовою особою Клієнта; |
| **"Representatives"** means a party's officers, directors, employees, agents, representatives, professional advisers and Third Party Service Providers; | **«Представники»** означають службовців, директорів, працівників, агентів, представників, професійних консультантів сторони та інших постачальників послуг; |
| **"Security Incident"** means an incident whereby the confidentiality of Disclosing Party Personal Data within Receiving Party's custody or control has been materially compromised so as to pose a reasonable likelihood of harm to the Data Subjects involved; | **«Інцидент інформаційної безпеки»** означає інцидент, через який конфіденційність Персональних даних Розкриваючої Сторони, в процесі їх зберігання або контролю Одержуючою Стороною, була суттєво порушена до виникнення обґрунтованого ризику заподіяння шкоди Суб'єктам відповідних даних; |

**"Third Party Service Provider"** means a third party reasonably selected by the Receiving Party or its Affiliate to provide services to or for the benefit of the Receiving Party, and who is not a Payment Infrastructure Provider. Examples of Third Party Service Providers include technology service providers, business process outsourcing service providers and call center service providers; and

**«Інший постачальник послуг»** означає третю сторону, доцільно обрану Одержуючою Стороною або її Афілійованою особою, для надання послуг Одержуючій Стороні або на її користь, і яка не є Постачальником платіжної інфраструктури. Приклади Інших постачальників послуг включають постачальників технічних послуг, постачальників аутсорсингових послуг бізнес-процесу та постачальників послуг колл-центру; і

# LOCAL CONDITIONS
# МІСЦЕВІ УМОВИ ДЛЯ ВЕДЕННЯ РАХУНКІВ

These Local Conditions for Accounts held and Services provided JSC "Citibank" in Ukraine, supplement and/or amend, and are to be read together with the Master Account and Service Terms or any other terms and conditions that may be in effect ("MAST"); Confidentiality and Data Privacy Conditions ("CDPC"); Cash Management User Guide ("UG"); and, if applicable, Regulatory Disclosures, Declarations, and Representations ("RDDR"). If there is a conflict between the MAST, CDPC, Local Conditions, UG and the RDDR, the RDDR will prevail. These Local Conditions, the MAST, CDPC UG, and RDDR may be updated from time to time with general applicability to customers and upon prior written notice to Customer.

Ці Місцеві умови для ведення Рахунків та надання Послуг АТ "Сітібанк" в Україні, з доповненнями та/або змінами, застосовуються разом з чинними Генеральними умовами обслуговування рахунку та надання послуг або будь-якими іншими чинними правилами (надалі – ГУ) ; Умовами про конфіденційність та секретність даних (надалі - УК); Довідники з управління грошовими коштами (надалі - ДУГК); та, якщо застосовно, Нормативним розкриттям інформації, заяв та представлення інформації " Regulatory Disclosures, Declarations, and Representations " (НР). Якщо існує конфлікт між ГУ, УК, Місцевими умовами, КУГК та НР, положення НР будуть переважати. Ці Місцеві умови, ГУ, УК, КУГК та НР можуть періодично оновлюватися з загальним застосуванням для клієнтів та після попереднього письмового повідомлення Клієнту.

## BANKING SECRECY

The Bank and the Customer agree that the definition of "Confidential Information" provided in CDPC shall for all purposes of the Agreement include, without limitation, any and all information defined as "banking secrecy" pursuant to applicable laws of Ukraine.

## БАНКІВСЬКА ТАЄМНИЦЯ

Банк та Клієнт погоджуються, що визначення терміну «Конфіденційна Інформація», наведене в УК, для усіх цілей цього Договору включатиме, без обмеження, будь-яку інформацію, яка є «банківською таємницею» згідно законодавства України.

## AMENDMENTS

The Bank may send to the Customer a written offer to amend the standard Terms. If the Customer does not provide to the Bank a written objection regarding proposed by the Bank amendments within 30 (thirty) calendar days from the date of sending of relevant Bank's notice, such amendments shall be considered as agreed by the Customer (silent consent) and will be effective after the expiry of the above-mentioned 30 (thirty) days period. If the Bank receives Customer written objections within 30 (thirty) calendar days from the date of sending of relevant Bank's notice, then the Bank shall have a right to unilaterally terminate the Agreement and close the Accounts.

## ЗМІНИ

Банк може надіслати Клієнту письмову пропозицію про внесення змін до Стандартних умов. У разі неподання Клієнтом письмових заперечень до Банку щодо запропонованих Банком змін протягом 30 (тридцяти) календарних днів з дати відправлення відповідного повідомлення Банку, такі зміни вважаються погодженими Клієнтом (мовчазна згода) та набирають чинності після закінчення вище вказаного 30 (тридцяти) денного строку. У випадку отримання Банком письмових заперечень Клієнта протягом 30 (тридцяти) календарних днів з дати відправлення відповідного повідомлення Банк має право в односторонньому порядку розірвати цей Договір та закрити Рахунки.

## PROCEDURE OF ACCOUNT CLOSING AND TERMINATION OF THE AGREEMENT

The Bank or the Customer may each unilaterally terminate the Agreement and close an Account or terminate all or part of any Service for any reason upon written notice, provided that in case of closure of the Account by the Customer it shall submit a duly executed account closure application.

## ПОРЯДОК ЗАКРИТТЯ РАХУНКУ ТА РОЗІРВАННЯ ДОГОВОРУ

Банк чи Клієнт можуть в односторонньому порядку розірвати Договір та закрити Рахунок або припинити надання будь-яких Послуг повністю або частково з будь-яких підстав шляхом надсилання письмового повідомлення, за умови, що у випадку закриття Рахунку Клієнтом останній повинен надати належним чином підписану заяву про закриття рахунку.

# Довідник з управління грошовими коштами

# Україна

Затверджено Правлінням АТ «СІТІБАНК»

**Протокол № 535 від 23 листопада 2018р.**

Treasury and Trade Solutions

# Зміст

# I. Передмова

Дякуємо, що для потреб Вашого бізнесу Ви обрали Казначейські та комерційні рішення Сіті (TTS) по управлінню грошовими коштами. Метою даного Довідника з управління грошовими коштами є надання клієнтам інструкцій, що містять докладну інформацію про послуги, які доступні клієнтам Банку. Зі змістом Довідника з управління грошовими коштами слід ознайомитись разом з умовами Банку, що регулюють обслуговування рахунку. У цьому довіднику, поняття «Сіті» та «Банк» використовуються як взаємозамінні. Цей довідник може час від часу оновлюватися, і про будь-які зміни буде повідомлено через наші звичайні засоби зв'язку.

# II. Послуги переказу коштів

## A. Види переказу коштів в Україні

- Перекази між рахунками «Сіті»: перекази коштів між рахунками клієнтів «Сіті» в Україні
- Місцеві перекази коштів: внутрішні електронні перекази коштів та електронні запити на списання коштів в режимі близькому до реального часу, оброблені Системою електронних Платежів (СЕП), яка підтримує перекази як великих, так і невеликих сум.
- Міжнародні перекази коштів: надають можливість клієнтам «Сіті» здійснювати міжнародні перекази в широкому діапазоні валют у формі вихідних електронних переказів

## B. Відправка платежу

1. Клієнт надсилає в «Сіті» платіжну інструкцію, оформлену відповідно до ринкових стандартів, через сервіси електронного банкінгу «Сіті», що були узгоджені на етапі підключення послуги, включаючи CitiDirect BE® та CitiConnect®
2. «Сіті» звіряє підписи на платіжній інструкції з підписами, що містяться у картці із зразками підписів, на відповідність, що може також включати перевірку по телефону. Банк не здійснюватиме обробку інструкції у випадку, якщо підпис не пройшов перевірку.
3. «Сіті» направляє інструкцію до СЕП для подальшої обробки.
4. СЕП направляє інструкцію банку отримувача коштів.
5. Банк отримувача зараховує кошти на рахунок отримувача.

Не існує жодних обмежень на суми оброблених транзакцій або на цілі здійснення платежу (комерційний, податковий, грошовий ринок тощо) за винятком виплати заробітної плати, що підлягає перевірці сплати податків перед виконанням, та інших регулярних платежів, які можуть бути предметом валютного регулювання.

Примітка: Банк буде діяти згідно з вимогою Клієнта відкликати, скасувати або змінити платіжну інструкцію, якщо це не заборонено законодавством України.

Якщо на рахунку Клієнта не вистачає коштів, Банк повертає платіжне доручення Клієнту. Банк не виконує часткові платежі.

## C. Подовження операційного дня для Клієнта

### Графік проведення платежів

| | **Термін завершення банківських операцій (місцевий час)** | **Дата валютування** |
|---|---|---|
| Місцеві перекази | 16:00 | Д |
| Переказ іноземної валюти | 11:00 | Д |
| Переказ між рахунками «Сіті» | 18:00 | Д |
| Зарплатні платежі | 16:00 | Д |

У виняткових випадках для клієнтів, які потребують подовження операційного банківського дня, можуть бути встановлені подовжені терміни завершення банківських операцій згідно окремих тарифів.

Клієнти повинні повідомити свого представника по обслуговуванню клієнтів про приблизний обсяг та кількість платежів, що підлягають обробці після звичайного часу завершення банківських операцій (16:00 для гривневих платежів та 12:00 для платежів в іноземній валюті). Подовжений термін завершення банківських операцій дійсний тільки для дня, коли подається запит. Якщо клієнти потребують подовженого терміну завершення банківських операцій більше одного дня, вищезазначене повідомлення повинно надсилатися «Сіті» кожного дня.

# III. Послуги вхідних платежів

## A. Отримання платежу

1. СЕП направляє інструкцію до «Сіті» відповідно до місцевих правил переказу коштів.
2. «Сіті» кредитує рахунок Клієнта.

Будь-які відмови або повернення коштів, ініційовані «Сіті», будуть повернуті на рахунок платника без виконання. Платнику сповіщається причина повернення.

## B. Послуги інкасації готівкових коштів

«Сіті» пропонує послуги інкасації готівкових коштів за допомогою окремого постачальника послуг. Послуги включають в себе наступне:

- Інкасація готівкових коштів: Збір банкнот та монет із приміщень Клієнта у попередньо узгоджений час для доставки до центрів інкасації та перерахунку
- Обробка готівкових коштів: Перерахунок та обробка (сортування та упаковка) інкасованих грошових коштів в призначених центрах перерахунку готівкових коштів та зарахування на рахунок Клієнта.

### Процес інкасації готівкових коштів

1. Клієнт та постачальник послуг повинні підписати угоду, що містить наступну інформацію:
   - Фактична адреса/коди місць інкасації Клієнта.
   - Графік інкасації грошових коштів - дні та час інкасації готівкових коштів.
   - Ім'я та контактний телефон уповноваженого представника Клієнта
   - Ім'я та контактний телефон уповноваженого представника постачальника послуг
   - Ціна, узгоджена з постачальником послуг
2. Клієнт заповнює установлену форму «Сіті» для налаштування послуги інкасації та обирає спосіб оплати послуг: автоматичне списання коштів з рахунку або оплата постачальнику послуг згідно рахунку.
3. Клієнт готує грошові кошти для інкасації до прибуття постачальника послуг.
   a. Грошові кошти повинні бути перераховані, відсортовані за номіналом, банкноти обв’язані та монети вкладені в мішечки для монет. Не дозволяється проводити обандеролювання або обв’язування банкнот, використовуючи невірну класифікаційну стрічку, незважаючи на номінальну вартість, написаною на стрічці від руки.
   b. Зношені банкноти сортуються окремо.
   c. Перед вкладенням готівки у сумку, уповноважена особа Клієнта (як зазначено в анкеті Клієнта) зобов’язана заповнити комплект бланків (супровідну відомість, накладну і копію супровідної відомості) до кожної сумки. Підписані копії повинні бути

опломбовані в сумці так, щоб пломба знаходилась якомога ближче до вузла. Кінці шпагату від зав'язаного вузла в пазу пломби повинні мати довжину не більше двох сантиметрів.

d. Постачальник послуг не прийме опломбовану сумку з готівкою, якщо сумка пошкоджена, розірвана, відбиток на пломбі нечіткий, або якщо є розбіжність між сумою, написаною цифрами, та сумою, написаною словами в доданих документах.

e. Клієнт зобов'язаний надати безперешкодну, добре освітлену та безпечну зону доступу для інкасації готівкових коштів.

4. Призначеного постачальника послуг зустрічають та супроводжують до місця інкасації готівкових коштів.

5. Клієнт перевіряє особу представника постачальника послуг (ідентифікаційний номер, довіреність та перепустку), робить відповідні помітки в реєстраційній картці та засвідчує, що підпис представника постачальника послуг співпадає з підписом на службовому посвідченні та довіреності.

6. Після інкасації готівкових коштів, представник постачальника послуг підписує супровідну відомість, яка підтверджує отримання сумки.

7. Представник доставляє грошові кошти до приміщень постачальника послуг для підрахунку готівкових коштів.

8. Грошові кошти перевіряються на дефекти, підробки та неприйнятні помітки та підраховуються. Сума, справжність та стан грошових банкнот та монет перевіряються постачальником послуг.

9. Грошові банкноти або монети, які виявились підробленими, будуть розглядатися постачальником послуг відповідно до чинних законів та правил. Будь-які пов'язані з цим витрати або наслідки є відповідальністю Клієнта.

10. Якщо готівка зібрана до 13:00, кошти на рахунок Клієнта будуть зараховані того ж дня. Усі грошові кошти, зібрані після 13:00. або в неробочий день будуть зараховані на рахунок Клієнта до 11:00 наступного робочого дня.

## C. Послуги з приймання платежів

«Сіті» пропонує рішення для приймання платежів від фізичних осіб по всій Україні.

### Процес приймання платежів

1. Клієнт повинен відкрити додатковий поточний рахунок, який буде використовуватися лише для приймання платежів.

2. Клієнт надає платникам спеціальні попередньо надруковані платіжні доручення для здійснення платежу. Зразок платіжного доручення повинен бути підтверджений "Сіті" до того, як Клієнт надасть його платникам.

3. Платники здійснюють платежі за допомогою попередньо надрукованого платіжного доручення через банки-постачальники послуг.

4. Кошти будуть зараховані на рахунок Клієнта «Сіті» не пізніше наступного робочого дня після того, як постачальник послуг отримав платіж.

## D. Сервіс обліку рахунків дебіторів

Сервіс обліку рахунків дебіторів «Сіті» (ARMS) – файлове рішення, що полягає у комбінуванні інструментів та методів передачі інформації із збагаченням деталей операції додатковою інформацією, що, у свою чергу, допомагає створювати стандартизовані звіти та автоматизувати реконсиляцію рахунків дебіторів.

### Консолідація

ARMS консолідує дані по вхідним платежам у стандартизовані звіти. Стандартизований звіт допомагає розпізнати та зіставити ключові дані з деталей платежів, щоб полегшити отримання платежів та їх реконсиляцію. «Сіті» підтримує як зручні для розуміння людиною, так і звіти та файли, що зчитуються машиною, для полегшення обробки дебіторської заборгованості клієнтів.

Процедура консолідації полягає у наступному:

1. «Сіті» отримує вхідний платіж від платника та зараховує платіж на рахунок Клієнта.
2. На основі узгодженого способу оплати, сервісу з обміну інформацією та параметрів рахунку, «Сіті» отримує дані про транзакції і надсилає їх у внутрішнє інформаційне сховище.
3. «Сіті» стандартизує дані, що містяться в транзакції.
4. «Сіті» створює звіти у попередньо узгоджений час і надсилає звіти або файли за допомогою узгодженого електронного сервісу з обміну інформацією, CitiDirect BE® або CitiConnect®

### Розширення даних

«Сіті» збагачує якість консолідованих даних про оплату за допомогою автоматизованої звірки даних.

Процес звірки ґрунтується на таблицях з даними, що надаються Клієнтом. Доступні наступні види звірки:

- Визначення платника – до деталей вхідних платіжних операцій із бібліотеки платників Клієнта додається інформація про платника. Це може включати унікальний ідентифікатор платника, ім'я або іншу необхідну інформацію про платника.
- Звірка даних платника згідно інформації від Клієнта, що полягає у розширенні вхідних платіжних операцій платіжною інформацією, яка надається Клієнту від платника.

Процедура розширення даних полягає в наступному:

1. Клієнт готує свої файли бібліотеки і передає їх через узгоджений електронний сервіс з обміну інформацією - CitiDirect BE® або CitiConnect®.
2. «Сіті» надсилає електронне повідомлення Клієнту, підтверджуючи отримання файлу бібліотеки.
3. Коли «Сіті» отримує вхідний платіж від платника, платіж обробляється та зараховується на рахунок Клієнта.
4. Потім дані платежу передаються в сховище даних через сервіс консолідації.
5. Як тільки процедура консолідації завершена, «Сіті» починає реконсиляцію даних, використовуючи доступні відповідні ключі/ідентифікатори.

6. Якщо ідентифікатори збігаються, «Сіті» додає до деталей платежу інформацію з бібліотеки Клієнта.

7. Якщо ідентифікатори не збігаються, «Сіті» надсилає сповіщення Клієнту для подальшої роботи з даним виключенням.

8. Після завершення реконсиляції, «Сіті» створює звіти у попередньо узгоджений час і передає звіт чи файли через узгоджений електронний сервіс з обміну інформацією - CitiDirect BE® або CitiConnect®.

### Реконсиляція рахунків-фактур

Реконсиляція рахунків-фактур - це послуга на основі правил, згідно яких відбувається звірка платежів, що зараховуються «Сіті» на рахунки Клієнта, із сумами платежів, що містяться у файлі, що надається Клієнтом.

Процедура реконсиляції рахунку-фактури наступна:

1. Клієнт готує бібліотеку рахунків, що очікують оплати, та передає файл за допомогою узгоджених електронних сервісів з обміну інформацією - CitiDirect BE® або CitiConnect®.

2. «Сіті» надсилає підтвердження електронною поштою про отримання даних бібліотеки Клієнта.

3. Коли «Сіті» отримує вхідний платіж від платника, він обробляється та зараховується на рахунок Клієнта «Сіті».

4. Потім дані про оплату передаються до внутрішнього сховища даних через сервіс консолідації.

5. Під час реконсиляції, деталі платежу скануються на предмет наявності в них ідентифікаторів, що використовуються як основний ключ для того, щоб отримати список неоплачених рахунків з бібліотеки.

6. Згідно з узгодженими правилами, «Сіті» додає інформацію щодо суми навпроти неоплаченого рахунку.

7. «Сіті» створює звіти та розширює дані як щодо повністю звірених сум, так і тих, що були звірені частково.

8. «Сіті» готує звіти у попередньо узгоджений час і надсилає звіт чи файли по узгодженому електронному сервісу з обміну інформацією - CitiDirect BE® або CitiConnect®.

# IV. Інші умови

Клієнт самостійно оцінює юридичні, регулятивні, податкові та бухгалтерські наслідки надання послуг.

Час від часу Банк надає Клієнту тарифи, процедури, вимоги, довідники, посібники та інші матеріали, що описують процедури, вимоги та обмеження щодо використання послуг.

Обробка вхідних та вихідних платежів регулюється правилами, встановленими відповідною платіжною системою. Крім того, даний Довідник відображає операційні процедури «Сіті». «Сіті» та клієнти «Сіті» повинні дотримуватися правил платіжних систем та операційних процедур, про які йдеться в даному довіднику.

Після заповнення Клієнтом та доставки до Банку відповідних реєстраційних форм, Банк надаватиме послуги по обслуговуванню рахунків Клієнта через систему Клієнт-Інтернет-Банк, використовуючи комплексну систему обробки та передачі електронних розрахункових документів та/або інших інструкцій, відповідно до вимог законодавства України та умов Угоди (як визначено у Заяві на відкриття рахунку), а також включаючи ці зведені процедури безпеки. Права, зобов'язання, відповідальність сторін та врегулювання спорів щодо використання системи Клієнт-Інтернет-банк визначаються в Угоді (в тому числі у цих Процедурах).

Система «Клієнт-Інтернет-Банк» означає систему CitiDirect BE та її мобільні додатки CitiDirect BE Mobile та CitiDirect BE Tablet, а також будь-які модифікації та зміни цієї системи, які Банк може застосувати в майбутньому.

Для рахунків Клієнта, що зареєстрований в Україні, функція Адміністратора системи здійснюється Банком. Ролі та обов'язки Адміністратора системи наведено в Розділі V (А) цього Довідника. Клієнт не вказує своїх Адміністраторів системі в жодній реєстраційній формі.

Будь-яка інструкція на здійснення переказу коштів з рахунку Клієнта, що зареєстрований в Україні, повинна бути авторизована у CitiDirect BE користувачем системи, що має повноваження на розпорядження рахунком відповідно до картки із зразками підписів. За необхідності, рівень підпису відповідно до карки із зразками підписів може прирівнюватись до права створення платежу, його відправки або авторизації.

# V. Консолідовані процедури безпеки TTS

Як зазначено в розділі «Повідомлення» Генеральних умов обслуговування рахунку та надання послуг (або інших застосовних умов використання рахунку) («MAST»), що були укладені між Клієнтом та Банком, нижче наведено опис процедур безпеки («Процедури»), що використовуються TTS «Сіті» по відношенню до таких послуг або сервісів з обміну інформацією.

- CitiDirect BE® (включаючи електронне управління банківськими рахунками (eBAM), TreasuryVision® та WorldLink®)
- Технології голосового розпізнавання IVR[1]
- Електронна пошта/факс з Банком, за винятком інструкцій, що вимагають ручного відправлення (MIFT)
- CitiConnect®
- Інші місцеві електронні канали передачі даних

Наявність послуг або сервісів з обміну інформацією може відрізнятись в залежності від ринку. Ці процедури можуть час від часу оновлюватись та надаватись Клієнту електронним або іншим способом. Продовження використання Клієнтом будь-яких із вищезазначених послуг або сервісів з обміну інформацією після отримання інформації про оновлені Процедури (що може включати, але не обмежується, публікацією оновлених процедур у CitiDirect BE щодо послуг або сервісу з обміну інформацією) означає прийняття Клієнтом таких оновлених процедур. Ці процедури мають бути прочитані разом з MAST, MAST може час від часу змінюватися. Визначення, вказані з великої літери, які не визначені інакше у цьому документі, мають значення, що визначене MAST.

## A. Роль та відповідальність Адміністратора системи[2]

Для програм, доступних у CitiDirect BE®, Банку необхідні дві окремі особи, щоб вводити та затверджувати інструкції; отже, потрібно мінімум два Адміністратора системи. Будь-які два Адміністратора системи, діючи спільно, можуть надавати інструкції та/або підтвердження через канали зв'язку щодо будь-якої функції Адміністратора системи або, для полегшення комунікації – через Інтернет. Будь-які такі Повідомлення, затверджені двома Адміністраторами системи, будуть прийняті та оброблені відповідно до правил Банку. Банк рекомендує призначити щонайменше трьох Адміністраторів системи для забезпечення безперервної роботи. Клієнт призначає своїх Адміністраторів системи у Формі підключення TTS сервісів з обміну інформацією. Адміністратор системи Клієнта також може виступати в якості Адміністратора системи для третіх осіб (наприклад, афілійованої особи Клієнта) та здійснювати всі необхідні дії (включаючи призначення користувачів для рахунку(-ів) третьої особи), без будь-якого додаткового призначення, якщо така третя особа підписує Форму універсального доступу (або іншу таку форму дозволу, що приймається банком), що надає Клієнту право доступу до свого рахунку(-ів). Це стосується лише рахунку(-ів), на який (які) розповсюджується відповідний дозвіл.

[1] *Опція не доступна в Україні*

[2] *Функція Адміністратора системи на сьогодні не доступна для прямого доступу до рахунків в Україні, крім випадків, коли клієнт, що зареєстрований за межами України, створює користувачів системи для права перегляду українських рахунків*

Роль Адміністратора системи включає, але не обмежується, наступними функціями:

1. Встановлення та підтримка доступу та прав користувачів, у тому числі самих Адміністраторів системи, включаючи такі дії:

   (a) створення, видалення або зміна облікових записів користувачів та наданих прав (зверніть увагу на те, що ім'я користувача повинно відповідати ідентифікаційним документам)

   (b) створення профілів доступу, які визначають функції та дані, доступні для різних користувачів, і

   (c) створення або видалення облікових даних користувача

2. Створення та зміна записів у бібліотеках Клієнта (наприклад, шаблони платежів

3. Зміна маршруту авторизації платежу[3]

4. Визначення облікових даних динамічного пароля або інших облікових даних доступу до системи або паролів користувачів Клієнта

5. Інформування Банку у разі підозри компрометації безпеки

6. Крім іншого, Адміністратори системи встановлюють ліміти для користувачів по транзакціям та продуктам, до яких користувач має доступ. Ці ліміти не відслідковуються та не перевіряються Банком; Клієнт самостійно слідкує за такими лімітами відповідно до своїх внутрішніх політик та вимог, які включають, але не обмежуються, лімітами, встановленими рішеннями Правління або іншим аналогічним документом.

Для роботи з **додатком eBAM**[4] необхідні наступні посади:

Початкова установка eBAM вимагає призначення трьох адміністраторів безпеки та одного корпоративного секретаря. Дві окремі старші адміністративні ролі діють спільно для створення користувачів та надання їм повноважень/ прав доступу до даних та робочих процесів. Ці механізми не контролюються та не перевіряються Банком; робочі процеси та дії користувачів контролюються Клієнтом для забезпечення дотримання політик, вимог та рівнів авторизації та затвердження Клієнта (і власників рахунків), включаючи, але не обмежуючись тими, що встановлені Радою директорів Клієнта (і власників рахунків) або еквівалентним керівним органом.

Для eBAM потрібні такі ролі:

1. **Адміністратор безпеки:** виконує функції, описані в (1) a-c вище, в рамках повноважень Адміністратора системи

2. **Корпоративний секретар:** гарантує, що робочі процеси, користувачі, яким надана роль Уповноваженого авторизатора, і їх закріплення за робочими процесами відповідають

[3] *Для інструкцій на переказ коштів з українських рахунків Банком вимагається наявність двох окремих користувачів для створення та авторизації інструкції. За необхідності, рівень підпису відповідно до карки із зразками підписів може прирівнюватись до права створення платежу, його відправки або авторизації.*

[4] *Додаток eBAM не використовується в Україні*

внутрішнім правилам, вимогам, рівням авторизації та дозволам, встановленим Радою директорів Клієнта (і Власниками рахунків) або еквівалентним керівним органом

3. **Уповноважений авторизатор:** має широкі повноваження для виконання та авторизації робочого процесу

4. **Ініціатори запиту:** це особи, уповноважені здійснювати адміністративні задачі, такі як введення запитів на управління рахунками та авторизаторами в додатку eBAM

Адміністратор безпеки, Корпоративний секретар та Уповноважений авторизатор несуть відповідальність за:

a) Визначення та керування налаштуваннями ієрархії та керування місцем/процесом, наприклад, встановлення робочих процесів та призначення користувачів та рівнів схвалення

b) Створення додаткових старших управлінських ролей та призначення на них користувачів (які можуть бути або не є співробітниками Клієнта)

c) Інформування Банку, якщо є підстави підозрювати, що безпека або конфіденційність будь-яких даних про користувачів (включаючи старші адміністративні ролі) були порушені або скомпрометовані

d) За необхідності, заповнення, зміну, затвердження та/або доповнення форм на підключення Клієнта, які час від часу можуть обґрунтовано вимагатись Банком у зв'язку з наданням Клієнту послуг та/або продуктів

## B. Засоби автентифікації

Процедури описують певні засоби перевірки справжності ("Засоби автентифікації"), які задіяні для виключної ідентифікації та перевірки повноважень Клієнта та/або будь-якого його користувача, як правило, за допомогою таких механізмів, як пари ID користувача/пароль, цифрові сертифікати та токени безпеки (що використовуються через апаратне або програмне забезпечення), які створюють динамічний пароль для доступу до служб або сервісів передачі даних кожного разу, коли Клієнт або користувач підключаються до систем або у разі само автентифікації. Будь ласка, зауважте, що доступність різних засобів автентифікації відрізняється в залежності від місцевих умов.

Адміністратори системи та усі користувачі, які хочуть (a) створювати або затверджувати транзакції (і чий профіль користувача дозволяє їм це робити) і/або (b) отримати доступ до систем відповідно до повноважень, повинні використовувати наявні засоби автентифікації (які, як зазначено вище, можуть оновлюватись часу від часу).

Наступні засоби автентифікації можуть бути доступними для доступу до вищезазначених служб або каналів передачі даних в поєднанні з ID користувача[5]:

[5] *За замовчуванням в Україні засобом автентифікації є Токен: Відповідь на запит. Використання інших засобів автентифікації має бути узгоджене з Банком.*

| **Засіб аутентифікації** | **Опис** |
|---|---|
| Токен: Відповідь на запит | (i) мобільний додаток на основі програмного токену (наприклад, MobilePASS) або (ii) фізичний токен (наприклад, SafeWord Card, Vasco), які в обох випадках використовуються для створення динамічного пароля після автентифікації за допомогою 4-значного PIN-коду. При доступі до CitiDirect BE® система створює запит, а токен, що використовується, створює код відповіді, що вводиться у систему. |
| Токен: Одноразовий пароль | (i) мобільний додаток на основі програмного токену (наприклад, MobilePASS) або (ii) фізичний токен (наприклад, SafeWord Card, Vasco), який використовується для створення динамічного пароля після автентифікації за допомогою 4-значного PIN-коду. Цей динамічний пароль вводиться в систему для отримання доступу. |
| Одноразовий код по SMS | Динамічний пароль доставляється користувачеві через SMS, після чого користувач вводить динамічний пароль і захищений пароль для отримання доступу до системи |
| Голосовий одноразовий код | Динамічний пароль доставляється користувачеві через автоматичний голосовий дзвінок, після чого користувач вводить динамічний пароль і захищений пароль для отримання доступу до системи |
| Багатофакторна автентифікація | Динамічний пароль створюється за допомогою токена SafeWord Card або MobilePASS, після чого такий динамічний пароль вводиться разом із захищеним паролем для отримання доступу до системи. |
| Цифрові сертифікати | Цифровий сертифікат, виданий затвердженим центром сертифікації, використовується з метою автентифікації. Цифрові сертифікати використовують Механізм зберігання ключа і відповідний ПІН, і можуть бути видані IdenTrust, SWIFT (3SKey) або іншими узгодженими постачальниками. |
| Захищений пароль | Користувач вводить свій захищений пароль для доступу до системи. Захищений пароль, як правило, обмежує можливості користувача в системі, наприклад, інформацію можна переглядати, але можливість здійснити транзакцію відсутня. |
| Система інтерактивної усної відповіді ("IVR") та електронна пошта | Користувачам, які зв'язуються з банком, буде запропоновано ввести PIN-код або надати іншу інформацію для підтвердження авторизованого доступу по телефону або електронною поштою. |
| Факс | Підписи на кореспонденції, що отримується Банком, за винятком запитів MIFT, будуть звірені з підписами, що містяться в рішенні правління Клієнта. |
| MTLS | Протокол *Mandatory Transport Layer Security* (MTLS) створює захищений, приватний електронний зв'язок між банком та зовнішньою стороною. Електронне повідомлення, відправлене за допомогою цього каналу, надсилається через Інтернет через зашифрований канал TLS, що створюється під час підключення. |
| Безпечний PDF | Зашифровані електронні листи доставляються до звичайної поштової скриньки як документ PDF, який відкривається шляхом введення особистого пароля, і, як саме повідомлення, так і всі додані файли шифруються. Приватний пароль може бути створений після отримання першого захищеного електронного листа. |

Щоб дізнатись більше про будь-який з цих засобів автентифікації, перегляньте сторінку *Login Help* довідки в CitiDirect BE®:
(https://portal.citidirect.com/portalservices/forms/loginHelp.pser)

Для CitiConnect®[6]:

- Якщо Клієнт вирішить використовувати загальнодоступне інтернет-з'єднання для підключення до «Сіті», включаючи HTTPS, безпечний FTP та FTPS, Банк та Клієнт обмінюються сертифікатами безпеки, щоб забезпечити повністю зашифрований та захищений канал зв'язку і обміну повідомленнями. Банк прийматиме тільки ті Повідомлення, що надходять із шлюзу захищеного зв'язку Клієнта, використовуючи сертифікати безпеки, якими обмінялись Банк та Клієнт, і навпаки, Банк передаватиме Повідомлення тільки до шлюзу зв'язку Клієнта, використовуючи такі ж самі сертифікати безпеки.

- Якщо Клієнт вирішує використовувати CitiConnect® для SWIFT, то для будь-яких платіжних доручень та інструкцій, що стосуються SWIFT, включаючи зміну або скасування таких інструкцій, Процедури, які будуть використовуватися для перевірки того, що платіжне доручення або інструкція отримані від Клієнта та уповноваженої особи Клієнта, є такими, як це передбачено Договірною документацією SWIFT (оскільки така документація визначається SWIFT і час від часу може бути змінена або доповнена), що включає, без обмежень, її Загальні положення та умови та Опис послуги FIN або як зазначено в будь-яких інших умовах, які можуть бути встановлені SWIFT. Банк не несе відповідальності за будь-які помилки або затримки в системі SWIFT. Повідомлення до Банку мають бути надані у форматі та такого типу, які необхідні та визначені SWIFT.

- При використанні VPN, як Клієнт, так і Банк призначають єдину IP-адресу, з якої будуть надсилатися та/або отримуватися Повідомлення від Клієнта та Банка. Банк прийматиме тільки ті Повідомлення, що походять із зазначеної IP-адреси Клієнта, і навпаки, Банк передаватиме Повідомлення тільки на вказану IP-адресу Клієнта.

- Клієнт та Банк також можуть використовувати захищений апаратний модуль автентифікації додатково до автентифікації VPN. Це вимагає від Банку та Клієнта встановлення пристрою на серверах, призначених для зв'язку між Банком та Клієнтом.

Банк вимагає:

- Захист Клієнтом засобів аутентифікації, включаючи будь-які реєстраційні дані та/або сертифікати безпеки, що пов'язані з засобами автентифікації (разом «Реєстраційні дані») та забезпечення доступу та розповсюдження Реєстраційних даних лише уповноваженим особам Клієнта. Засоби автентифікації та пов'язані з ними Реєстраційні дані є методами, за допомогою яких Банк перевіряє походження Повідомлень, що надсилаються Клієнтом для Банку.

- Клієнт повинен вжити всіх необхідних заходів для захисту Реєстраційних даних. Відповідно, Банк наполегливо рекомендує, щоб Клієнт не передавав Реєстраційні дані будь-якій третій стороні.

В деяких юрисдикціях для отримання доступу для виконання визначених функцій від фізичних осіб (та їх відповідних Реєстраційних даних) вимагається пройти процедуру ідентифікації відповідно до вимог законодавства щодо протидії відмиванню коштів.

Банк розуміє, що у деяких випадках Клієнт може передати Реєстраційні дані третій стороні або постачальникам послуг (включаючи, але не обмежуючись, будь-якого постачальника з обробки заробітної плати), що визначені Клієнтом для доступу до Реєстраційних даних Клієнта (така третя сторона або постачальник послуг надалі -

*[6] Інструкції на переказ коштів, надані сервісом CitiConnect, потребують авторизації у CitiDirect BE користувачем, що має право розпорядження рахунком.*

«Уповноважена третя сторона») з метою доступу та використання будь-якого з банківських електронних каналів від імені Клієнта. У випадку, якщо Клієнт вирішить надати свої реєстраційні Уповноваженій третій стороні, Банк наполегливо рекомендує, щоб Клієнт приймав та гарантував, що будь-яка Уповноважена третя сторона буде вживати усі розумні заходи для захисту реєстраційних даних від розголошення будь-якому не уповноваженим співробітникам третьої сторони. Банк уповноважений приймати рішення щодо будь-якого Повідомлення, яке він отримує від Уповноваженої третьої сторони від імені Клієнта відповідно до цих процедур.

## C. Цілісність даних та захищені Повідомлення

- Клієнт буде передавати дані та іншим чином обмінюватися Повідомленнями з Банком, використовуючи Інтернет, електронну пошту та/або факс, які не обов'язково є безпечними системами зв'язку та доставки. Банк використовує провідні галузеві методи шифрування (визначені Банком), які допомагають забезпечити конфіденційність інформації та її цілісність під час передачі.

- Якщо Клієнт підозрює чи виявить технічний збій або будь-який неналежний доступ до сервісів Банку, каналів з'єднання або засобів автентифікації будь-якою особою (незалежно від того, уповноважена особа чи ні), Клієнт негайно повідомляє про це Банк. У випадку неправомірного доступу або використання уповноваженою особою, Клієнт повинен негайно вжити заходів для припинення доступу уповноваженої особи до послуг Банку або каналів з'єднання.

- Якщо Клієнт використовує форматування файлів, програмне забезпечення для шифрування (незалежно від того, надане Банком або третьою стороною) для підтримки форматування та розпізнавання даних та інструкцій Клієнта та діє відповідно до Повідомлень з «Сіті», то Клієнт буде використовувати таке програмне забезпечення лише для цілей, для якого воно була встановлено.

- Клієнт погоджується, що Банк може призупинити доступ Користувачів до послуг, які вимагають використання Реєстраційних даних (i) у разі підозри в несанкціонованому або шахрайському використанні Реєстраційних даних та/або (ii) для захисту Сервісві та/або Реєстраційних даних.

# VI. Прикінцеві положення

Дякуємо, що обрали Банківські операції та торгові рішення «Сіті» (TTS) для потреб, пов'язаних з управлінням грошовими коштами. Будь ласка, звертайтеся до вашого менеджера з питань відносин із «Сіті» у випадку будь-яких додаткових питань, які ви маєте відносно послуг TTS.

Банківські операції та торгові рішення
**citi.com/tts**

# Cash Management User Guide

## Ukraine

Approved by the Management Board of JSC “CITIBANK”

Minutes No.535 dated 23 November 2018

Treasury and Trade Solutions

citi

# Table of Contents

# I. Introduction

Thank you for choosing Citi's Treasury and Trade Solutions (TTS) for your cash management business needs. The objective of this Cash Management User Guide is to provide customers with a manual containing detailed information of services available to them and is to be read together with account terms and conditions. In this guide, Citi and Bank may be used interchangeably. This guide may be updated from time to time and any changes will be communicated through our regular channels.

# II. Payment Services

## A. Types of Payments Services in Ukraine

- Book Transfers: Transfers of funds between Citi accounts in Ukraine
- Domestic Funds Transfers: Near real-time domestic electronic funds transfers and electronic requests for debits processed via the System for Electronic Payments (SEP), which supports both high-value and low-value transfers.
- Cross Border Funds Transfers: Allow Citi customers to make international transfers in a wide range of currencies as outgoing telegraphic transfers

## B. Sending a Payment

1. The Customer sends a payment instruction to Citi, formatted to market standards and as outlined at the time the payment service was implemented via Citi e-banking channels, which include CitiDirect BE® and CitiConnect®
2. Citi will verify the signatures, which may include verification via telephone, against the signatures contained in the Signature Card. If a signature cannot be verified the instruction will not be processed by the Bank.
3. Citi forwards the instruction to SEP for further processing.
4. SEP forwards the instruction to the beneficiary bank.
5. The beneficiary bank credits the beneficiary account.

There are no restrictions on processed transaction amounts or the purpose of a payment (commercial, tax, money market, etc.) except for payroll payments, which are subject to a tax check before execution, and other regular payments, which may be subject for currency control check.

Note: The Bank will act on the Customer's request to recall, cancel or amend a payment instruction, unless prohibited by Ukrainian law.

If there are insufficient funds in the Customer's Account, the Bank will return the payment order to the Customer. The Bank does not execute partial payments.

## C. Customer Extended Cut-Off

### Standard Funds Availability Schedule for UAH

| | Cut Off time (Local) | Value Date |
|---|---|---|
| Domestic Wire | 4:00 p.m. | D |
| Foreign Currency Transfer | 11:00 a.m. | D |
| Book Transfer | 6:00 p.m. | D |
| Payroll | 4:00 p.m. | D |

In exceptional circumstances, customers who require an extended operating banking day for may establish late cut-off times for a separate fee.

Customers should inform their Customer Experience Representative of the approximate value and number of payments to be processed past normal cut-off (4:00 p.m. for UAH and 12:00 p.m. for foreign currency payments). An extended cut-off time is only valid for the particular day it is requested. If customers require extended cut-offs for more than one day, the above-mentioned notification must be sent to Citi each day.

# III. Receivables Services

## A. Receiving a Payment

1. SEP forwards the instruction to Citi based on the locally defined clearing cycle.
2. Citi credits the Customer's Account.

Any rejections or returns by Citi will be credited back to the payer account. The reason for the return is communicated to the payer.

## B. Cash Collection Services

Citi offers door-to-door cash collection and exchange using its dedicated service provider. The services include the following:

- Cash Collection**:** Pickup of physical currency notes and coins from the Customer's premises at a pre-agreed time for delivery to cash collection and counting centres.
- Cash Processing: Counting and processing (sorting and packaging) collected cash in designated cash counting centres and crediting to the Customer's Account.

### Cash Collection Process

1. The Customer and service provider must have a signed agreement covering the following:
    - Actual address/codes of Customer sites to be collected
    - Cash collection schedule – days and time of cash collection
    - Name and contact telephone number of the Customer's authorized representative
    - Name and contact telephone number of the service provider's authorized representative
    - The pricing agreed with the service provider
2. The Customer completes the Citi cash collection set-up form and selects direct billing or service provider billing.
3. The customer prepares the cash for collection prior to the service provider's arrival.
    a. Cash must be counted, sorted by face value, banknotes bundled, and coins placed in the coin sack. It is prohibited to band or bundle banknotes utilizing an incorrect denomination slip, regardless of the handwritten denomination.

b. Worn out banknotes should be separated.

c. Before placing the funds into the sealed container the Customer's authorized person (as specified in the Customer's Application Form) will complete a set of forms (accompanying sheet, consignation and copy of the accompanying sheet) for each bag. Signed copies should be sealed within the pouch so that the seal is located as close to the lock as possible. The entire twine from the knot to the end, which is tucked into a groove of the seal, should not be more than two centimeters long.

d. The service provider will not accept sealed cash containers if they are damaged, torn, have an illegible sealing mark, or contain a discrepancy between the sum written in digits and the sum written in words in the enclosed documents.

e. The Customer will provide an unobstructed, well-lit and secure access area for cash collection.

4. The appointed service provider is met and escorted to the cash collection area.

5. The Customer verifies the identity of the service provider's representative (ID, power of attorney document and attendance card), makes relevant notes in the registration card, and certifies that the signature of the service provider's representative matches that on the service certificate and power of attorney documents.

6. Upon collection of the cash, the service provider's representative signs the acceptance form confirming receipt of the package.

7. The representative delivers the cash to the service provider's cash counting facilities.

8. The cash is inspected for defective, counterfeit and unacceptable notes and counted. The amount, authenticity and condition of the currency notes and coins are verified by the service provider.

9. Currency notes or coins found to be counterfeit will be dealt with by the service provider according to applicable laws and regulations. Any related costs or consequences are the Customer's responsibility.

10. If cash is collected before 1:00 p.m., the Customer's Account will be credited on the same day. All cash collected after 1:00 p.m. or on a non-business day will be credited to the Customer's Account before 11:00 a.m. on the next business day.

## C. Mass Collection Services

Citi offers solutions for payment collection from individuals across Ukraine.

### Mass Collection Process

1. The Customer must open an additional current account to be used only for mass collection.
2. The Customer provides payers with a special pre-printed payment orders for payment initiation. Payment order draft must be confirmed by Citi before the Customer provides it to payers.
3. Payers will make payments using the pre-printed payment order via Service provider banks.
4. Funds will be credited to the Customer's Citi account not later than next working day after payment was received by Service provider.

## D. Account Receivables Matching Service (ARMS)

The Citi Accounts Receivable Matching Service (ARMS) is a file-based solution that combines a complete range of channels and instruments with enriched transaction data, allowing standardized reporting and, ultimately, straight through reconciliation.

### Consolidation

ARMS includes the consolidation of incoming payments data into standardized reporting. Standardized reporting helps to recognize and integrate key data points from the payment information to facilitate the receipt of payments and cash application. Citi supports both human- and machine-readable reports and files to help facilitate the Customer account receivables processing.

The consolidation procedure is as follows:

Citi receives an incoming payment from the payer and credits the payment into the Customer's Account.

1. Based on the agreed payment mode, channel and account parameters, Citi extracts the transaction data and delivers it to an internal data warehouse
2. Citi standardizes the data contained in the transactions.
3. Citi generates reports at the pre-agreed time and delivers the reports or files via the agreed Citi e-banking channel, CitiDirect BE® or CitiConnect®

### Data Enrichment

Citi enriches the quality of consolidated payment data through automated data matching.

The data matching process relies on the Customer providing specific data tables. The following types of data matching are available:

- Payer Matching, which involves enriching incoming payment transactions with additional payer information from the Customer's library of payers. This may include a unique Payer ID, name, or other relevant payer information.
- Payer Advice Matching, which involves enriching incoming payment transactions with payment information that is provided by the payer to the Customer.

The data enrichment procedure is as follows:

1. The Customer prepares its library data files and transmits them via the agreed Citi e-banking channel, CitiDirect BE® or CitiConnect®.
2. Citi sends an e-mail to the Customer confirming receipt of the library data file.
3. When Citi receives an incoming payment from a payer, the payment is processed and credited into the Customer's Account.
4. The payment data is then transferred to the data warehouse via the consolidation service.
5. As soon as the consolidation procedure is complete, Citi initiates the data matching procedure using available matching keys/identifiers.
6. If the identifiers match, Citi enriches the payment data with information from the Customer library.
7. If there is no match, Citi emails an alert to the Customer to take appropriate exception actions.
8. Once the data matching is completed, Citi generates reports at the pre-agreed time(s) and delivers the report or files via the agreed Citi e-banking channel, CitiDirect BE® or CitiConnect®.

### Invoice Reconciliation

Invoice reconciliation is a rules-based service that extracts payment data received by Citi into the Customer's account and applies the payment amount against a data file provided by the Customer.

The invoice reconciliation procedure is as follows:

1. The Customer prepares a library of unpaid items and transmits the file via the agreed Citi e-banking channel, CitiDirect BE® or CitiConnect®.
2. Citi emails the Customer contact, confirming receipt of the Customer library data.
3. When Citi receives an incoming payment from the payer, it is processed and credited into the Customer's Citi account.
4. The payment data is then transferred to the internal data warehouse via the consolidation service.
5. During invoice reconciliation, payment data is scanned for reconciliation identifiers and, using these identifiers as a primary key, a list of unpaid items is pulled from the unpaid items library.
6. Citi then applies the payment amount against the unpaid items using the conditions agreed.
7. Citi reports and enriches both full and partially reconciled items.
8. Citi generates reports at the pre-agreed time and delivers the report or files to the agreed Citi e-banking channel, CitiDirect BE® or CitiConnect®.

# IV. Other Considerations

The Customer will make its own assessment of the legal, regulatory, tax and accounting implications of the services.

From time to time, the Bank shall deliver to the Customer fee schedules, procedures, requirements, guides, manuals and other materials describing the procedures, requirements and limitations surrounding the use of the services.

The clearing of payments and receivables is governed by the rules set by the corresponding clearing system. Additionally, this User Guide reflects Citi's operating procedures. Both Citi and its customers must adhere to the clearing rules and operating procedures, as detailed in this guide.

Upon completion by the Customer and delivery to the Bank of the relevant onboarding forms, the Bank will provide services through the Client-Internet-Bank system on maintaining Accounts of the Customer using the complex system of processing and transmitting electronic settlement documents and/or other instructions in accordance with requirements of the Ukrainian legislation, and the terms of the Agreement (as defined in the Account Opening Form), including these Consolidated Security Procedures. The rights, obligations, liabilities of the parties, and dispute settlement provisions in relation to the use of the Client-Internet-Bank system are determined in the Agreement (including these Procedures).

The "Client-Internet-Bank" system shall mean CitiDirect BE system and its mobile applications, as well as any modifications and changes to this system, which may be applied by the Bank in the future.

For the on-shore accounts domiciled in Ukraine, the Security Manager function for the Customer will be performed by the Bank. Roles and responsibilities of the Security Manager function are outlined in Section V (A) of this User Guide. The Customer may omit the designation of its own Security Managers in any onboarding form.

Any instruction for funds transfer from a Ukraine-domiciled Customer account will be authorized in CitiDirect BE by a user with the authority to operate the account as per the signature sample card. Signature authority level as per the signature sample card may be aligned with payment input, payment release or authorization functionality, if required.

# V. TTS Consolidated Security Procedures

As referenced in the Communications section of the Master Account and Service Terms (or other applicable account terms and conditions) ("MAST") that has been entered into between the Customer and the Bank the following is a description of the security procedures ("Procedures") used by Citi Treasury and Trade Solutions in connection with the following Services or connectivity channels.

- CitiDirect BE® (including Electronic Bank Account Management ("eBAM"), TreasuryVision®, and WorldLink®)
- Interactive Voice Response ("IVR")[1]
- Email/fax with the Bank excluding Manually Initiated Funds Transfer (MIFT)
- CitiConnect®
- Other local electronic connectivity channels

Availability of the Services or connectivity channels will vary across local markets. These Procedures may be updated and advised to the Customer by electronic means or otherwise from time to time. Customer's continued use of any of the above noted services or connectivity channels after being advised of updated Procedures (which may include, but is not limited to, the posting of updated Procedures on CitiDirect BE in connection with the service or connectivity channel) shall constitute Customer's acceptance of such updated Procedures. These Procedures are to be read together with the MAST as such MAST may be amended from time to time. Capitalized terms not otherwise defined herein shall have the meanings ascribed to them in the MAST.

## A. Security Manager Roles and Responsibilities[2]

For the applications accessible in CitiDirect BE, the Bank requires two separate individuals to input and authorize instructions; therefore a minimum of two Security Managers are required. Any two Security Managers, acting in concert, are able to give instructions and/or confirmations through the connectivity channels in relation to any Security Manager function or in connection with facilitating our communication via the Internet. Any such Communications, when authorized by two Security Managers, will be accepted and acted on by the Bank. The Bank recommends the designation of at least three Security Managers to ensure adequate backup. The Customer shall designate its

[1] *IVR is not available in Ukraine.*

[2] *Security Manager Roles and Responsibilities currently do not apply for direct access to accounts domiciled in Ukraine, except where a non-Ukraine client is setting up users for view only access to Ukraine accounts. For the Ukrainian Customer accounts Security Manager function is performed by the bank . Please contact your Customer Service representative for further information.*

Security Managers on the TTS Channels Onboarding Form. A Security Manager of the Customer may also act as the Security Manager for a third party entity (for instance, an affiliate of the Customer) and exercise all rights relating thereto (including the appointment of users for that third party entity's Account(s)), without any further designation, if that third party entity executes a Universal Access Authority form (or such other form of authorization acceptable to the bank) granting the Customer access to its Account(s). This only applies in relation to Account(s) covered under the relevant authorization.

The Security Manager function includes, but is not limited to:

1. Establishing and maintaining the access and entitlements of users (including the Security Managers themselves), including activities such as:
    a. creating, deleting or modifying User Profiles (including Security Manager Profiles) and entitlement rights (please note that user name must align with supporting identification documents)
    b. building access profiles that define the functions and data available to various users, and
    c. enabling and disabling user log-on credentials
2. Creating and modifying entries in Customer maintained libraries (such as preformatted payments and beneficiary libraries) and authorizing other users to do the same
3. Modifying payment authorization flows3
4. Allocating dynamic password credentials or other system access credentials or passwords to the Customer's users
5. Notifying the Bank if there is any reason to suspect that security has been compromised.
6. Security Managers also assign transaction limits to users for those Bank products to which the Customer has access. These limits are not monitored or validated by the Bank; Customer should monitor these limits to ensure in compliance with Customer's internal policies and requirements, including but not limited to, those established by Customer's Board of Directors or equivalent.

Specifically related to the **eBAM Application,** the following roles are required [4]:

---

*[3] For payments initiated on Ukraine accounts in CitiDirect BE the Bank requires two separate users to input and authorise instructions. Signature level as per signature sample card may be aligned with payment input, payment release or authorization functionality as required.*

*4 eBAM Application is not available in Ukraine*

The initial set-up on the eBAM Service requires the designation of three Security Officers and one Corporate Secretary. Two separate Senior Administrative Roles act in concert as maker/checker to set up and assign User function/data entitlements and Workflows. These arrangements are not monitored or validated by Bank; Workflows and User activity are monitored by the Customer to ensure compliance with Customer's (and Account Owners') internal policies, requirements, and authorization and approval levels, including but not limited to those established by the Customer's (and Account Owners') Board of Directors or equivalent governing body.

The following roles are required for the eBAM Service:

1. **Security Officer:** fulfills functions described in (1) a-c above within the roles of Security Managers

2. **Corporate Secretary:** ensures that Workflows, Users set up as Designated Authorizers, and their assignment to Workflows meet internal policies, requirements, authorization and approval levels, as established by the Customer's (and Account Owners') Board of Directors or equivalent governing authority

3. **Designated Authorizer:** have broad, senior authority to initiate and authorize Workflow activities

4. **Request Initiators:** are individuals authorized to perform administrative activities such as entering account and signer management requests into the eBAM system

The Security Officers, Corporate Secretary, and Designated Authorizers are responsible for:

a) Defining and administering hierarchy setup and site/flow control, such as establishing Workflows and identifying Users and levels of approval

b) Creating additional Senior Administrative Roles and appointing Users thereto (who may or may not be employed by the Customer)

c) Notifying Bank if there is any reason to suspect that security or confidentiality of any User (including Senior Administrative Roles) credentials has been breached or compromised

d) Where relevant, completing, amending, approving and/or supplementing such Customer implementation forms as may be reasonably requested by Bank from time to time in connection with the provision of services and/or products to Customer

## B. Authentication Methods

The Procedures include certain secure authentication methods ("Authentication Methods") which are used to uniquely identify and verify the authority of the Customer and/or any of its users typically through mechanisms such as User ID / password pairs, digital certificates, and security tokens (deployed via hardware or software) which generate a dynamic password used to access the services or connectivity channels each time the Customer or a user logs in or authenticates themselves. Please note that availability of the Authentication Methods described below varies based on local markets.

Security Managers and all users who want to (a) initiate or approve transactions (and whose User Profile permits them to do so) and/or (b) access the systems in accordance with entitlements must use the available Authentication Methods (which may be updated from time to time as described above).

The following Authentication Methods are available to access the above-noted services or connectivity channels in combination with a User ID[5]:

[5] *Token: Challenge Response is configured as the default authentication method for clients in Ukraine. Use of other authentication methods by Ukraine clients should be pre-agreed with the Bank.*

| Authentication Method | Description |
|---|---|
| Token: Challenge Response | Either a (i) mobile application based soft token (e.g. MobilePASS) or (ii) physical token (e.g. SafeWord Card, Vasco) which in each case is used to generate a dynamic password after authenticating with a 4 digit pin. When accessing CitiDirect BE®, the system generates a challenge, and a response passcode is generated by the utilized token and entered into the system. |
| Token: One-Time Password | Either a (i) mobile application based soft token (e.g. MobilePASS) or (ii) physical token (e.g. SafeWord Card, Vasco) which is used to generate a dynamic password after authenticating with a 4 digit pin. This dynamic password is entered into the system to gain access. |
| SMS One-Time Code | A dynamic password is delivered to a user via SMS, after which the user enters the dynamic password and a secure password to gain access to the system |
| Voice One-Time Code | A dynamic password is delivered to a user via an automated voice call, after which the user enters the dynamic password and a secure password to gain access to the system |
| MultiFactor Authentication | A dynamic password is generated via a SafeWord Card or MobilePASS token, after which such dynamic password is entered along with a secure password to gain access to the system. |
| Digital Certificates | A Digital Certificate issued by an approved certificate authority which is used for authentication. Digital Certificates utilize a Key Storage Mechanism and a corresponding PIN, and may be issued by IdenTrust, SWIFT (3SKey) or other agreed-upon providers. |
| Secure Password | A user enters their secure password to access the system. A Secure Password typically limits a user's capabilities on the system, such that information can be viewed and no transaction capabilities are enabled. |
| Interactive Voice Response ("IVR") & email | Users contacting the bank will be prompted to enter a PIN number or provide other information to validate authorized access over the phone or over email. |
| Fax | Correspondence received by the Bank, excluding MIFT requests, will be signature verified based on the information that is contained in the Customer's board resolution. |
| MTLS | Mandatory Transport Layer Security (MTLS) creates a secure, private email connection between the bank and the external party. An email transmitted sent using this channel is sent over the Internet through an encrypted TLS tunnel created by the connection. |
| Secure PDF | Encrypted emails are delivered to a regular mailbox as a PDF Document that is opened by entering a private password, both the message body and any attached files are encrypted. A private password can be set up upon receipt of the first Secure Email received. |

To learn more about any of these Authentication Methods, please refer to the Login Help page on CitiDirect BE®: (https://portal.citidirect.com/portalservices/forms/loginHelp.pser)

For CitiConnect®[6]:

- If the Customer chooses to use a public Internet connection to connect to Citi, including HTTPS, secure FTP, and FTPS, the Bank and the Customer will exchange security certificates to ensure both the communication channel and the messages exchanged are fully encrypted and protected. The Bank will only accept Communications originating from the Customer's secured communications gateway using the exchanged security certificates, and vice versa, and the Bank will only transmit Communications to the Customer's communication gateway using the exchanged security certificates.

- If the Customer chooses to use CitiConnect® via SWIFT, then for any payment orders and instructions involving SWIFT, including amending or cancelling such orders, the Procedures that will be used to authenticate that a payment order or instruction is that of the Customer and authorized by the Customer shall be those as provided for in the SWIFT Contractual Documentation (as such term is defined by SWIFT and as may be amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in any other terms and conditions that may be established by SWIFT. The Bank is not responsible for any errors or delays in the SWIFT system. Communications to the Bank are to be provided in the format and type required and specified by SWIFT.

- If using a VPN, both the Customer and the Bank will designate a single IP address from which Communications between the Customer and Bank will be sent and/or received. The Bank will only accept Communications originating from the Customer's designated IP address, and vice versa, and the Bank will only transmit Communications to the Customer's designated IP address, and vice versa.

- The Customer and the Bank may also use a Hardware Security Module Authentication to accompany VPN Authentication. This requires the Bank and the Customer each to install a device on the servers designated for Communications between the Bank and the Customer.

Any instruction for funds transfer delivered by CitiConnect® channel requires authorization of the instruction in CitiDirect BE® by the user with the authority to operate an account.

The Bank requires:

- Customer's safeguarding of the Authentication Methods including any log-on credentials and/or security certificates associated with the Authentication Methods (collectively, the "Credentials") and ensuring that access to and distribution of the Credentials are limited

[6] *Payment instructions for a Ukraine account delivered using CitiConnect require authorization of the instruction in CitiDirect BE® by a user with the authority to operate the account.*

only to authorized persons of the Customer. The Authentication Methods and associated Credentials are the methods by which the Bank verifies the origin of Communications issued by the Customer to the Bank.

- The Customer should take all reasonable steps to protect the Credentials. Accordingly, the Bank strongly recommends that the Customer does not share the Credentials with any third party.

Certain jurisdictions may require individuals (and their corresponding credentials) to be identified as compliant with applicable AML legislation requirements before granting access to perform certain functions.

The Bank understands that the Customer may, in some cases, wish to share the Customer's Credentials with a third party entity or service provider (including without limitation any third party payroll provider) designated by the Customer to have access to the Customer's Credentials (such third party entity or service provider shall be referred to herein as an "Authorized Third Party") for the purpose of accessing and utilizing any of the banks electronic channels on the Customer's behalf. In the event that the Customer elects to share its Credentials with an Authorized Third Party, the Bank strongly recommends that the Customer takes, and ensure that any Authorized Third Party takes, all reasonable steps to protect the Credentials from being disclosed to any non-Authorized Third Party personnel. The Bank is authorized to act upon any Communication that it receives from an Authorized Third Party on behalf of the Customer in compliance with these Procedures.

## C. Data Integrity and Secured Communications

- The Customer will be transmitting data to and otherwise exchanging Communications with the Bank, utilizing the Internet, email and/or fax, which are not necessarily secure communication and delivery systems. The Bank, utilizes industry leading encryption methods (as determined by the Bank), which help to ensure that information is kept confidential and that it is not changed during transit.

- If the Customer suspects or becomes aware of, a technical failure or any improper access to or use of the Bank's services, connectivity channels or the Authentication Methods by any person (whether an authorized person or not), the Customer shall promptly notify the Bank of such occurrence. In the event of improper access or use by an authorized person, the Customer should take immediate actions to terminate such authorized person's access to and use of the Bank's services or connectivity channels.

- If Customer utilizes file formatting, encryption software (whether provided by the Bank or a third party), to support the formatting and recognition of the Customer's data and

instructions and acts upon Communications with Citi, then the Customer will use such software solely for the purpose for which it has been installed.

- The Customer accepts that the Bank may suspend the access of the Users to the Services that require the use of the Credentials (i) in case of suspicion of unauthorized or fraudulent use of the Credentials and/or (ii) in order to safeguard the Services and/or Credentials.

# VI. Conclusion

Thank you for choosing Citi Treasury and Trade Solutions (TTS) for your cash management needs. Please feel free to contact your Citi relationship manager with any additional questions that you have regarding TTS services.

Treasury and Trade Solutions
**citi.com/tts**