

Security Procedures

Процедури безпеки

1. Introduction

Вступ

These “Security Procedures”, as referenced in the Communications section of the Master Account and Service Terms (“MAST”) (or other applicable account terms and conditions), are designed to authenticate the Customer’s log-on to the Bank’s connectivity channels and to verify the origination of Communications between Bank and Customer in connection with the following Services or connectivity channels (the availability of which may vary across local markets).

Як зазначено в розділі Зв’язок Основних положень та умов обслуговування рахунків (MAST) (або інших застосовних положень та умов рахунків), ці Процедури безпеки, призначені для підтвердження автентичності входу Клієнта до каналів зв’язку Банку та для перевірки походження зв’язку між Банком та Клієнтом стосовно таких Послуг або каналів зв’язку (доступність яких може відрізнятися на різних місцевих ринках).

- CitiDirect® (including WorldLink®)
CitiDirect® (включаючи WorldLink®)
- CitiConnect®
CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication (“SWIFT”)
Society for Worldwide Interbank Financial Telecommunication (SWIFT)
- Manual Initiated Funds Transfer (“MIFT”)
Переказ коштів, ініційований вручну (Manual Initiated Funds Transfer, MIFT)
- Interactive Voice Response (“IVR”)
Інтерактивна голосова відповідь (Interactive Voice Response, IVR)
- Email/Fax/Mail/Messenger/Phone with the Bank
Контакт з Банком за допомоги електронної пошти/факса/звичайної пошти/месенджера/телефона
- Other local electronic connectivity channels
Інші локальні електронні канали зв’язку

These Security Procedures are to be read together with the MAST and may be updated and advised to the Customer from time-to-time by electronic or other means, including but not limited to posting updates to the Security Procedures on CitiDirect. Unless otherwise provided by law, Customer’s continued use of any of the above noted Services or connectivity channels after being advised of updated Security Procedures shall constitute Customer’s acceptance of such updated Security Procedures. These Security Procedures cover the following:

Ці Процедури безпеки слід читати разом з MAST. Вони можуть час від часу оновлюватися та доводитися до відома Клієнта за допомогою електронних або інших засобів, включаючи, але не обмежуючись, публікацію оновлень до Процедур безпеки в CitiDirect. Якщо інше не передбачено законодавством, подальше використання Клієнтом будь-якої з вищезазначених Послуг або каналів зв'язку після отримання повідомлення про оновлені Процедури безпеки означає згоду Клієнта з такими оновленими Процедурами безпеки. Ці Процедури безпеки охоплюють наступне:

- A. Authentication Methods
Засоби автентифікації
- B. Customer Responsibilities
Обов'язки Клієнта
- C. Data Integrity and Secured Communications
Цілісність даних та захищені комунікації
- D. Security Manager and Related Functions
Менеджер з безпеки та пов'язані з ним функції

2. Authentication Methods *Методи автентифікації*

The Security 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 authorized by the Customer typically through one or a combination of mechanisms such as user ID/password pairs, digital certificates, biometrics, security tokens (deployed via hardware or software), seal/signature verification, and/or devices associated with the Authentication Methods (collectively, the "Credentials"). Authentication Methods and associated Credentials allow the Bank to verify the origin of Communications received by the Bank.

Процедури безпеки включають певні безпечні методи автентифікації (Методи автентифікації), які використовуються для унікальної ідентифікації та перевірки повноважень Клієнта та/або будь-якого його користувача, уповноваженого Клієнтом, як правило, за допомогою одного або комбінації таких механізмів, як пари ідентифікатор користувача/пароль, цифрові сертифікати, біометричні дані, токени безпеки (розгорнуті за допомогою апаратного або програмного забезпечення), перевірка печатки/підпису та/або пристрої, пов'язані з Методами автентифікації (разом - Облікові дані). Методи автентифікації та пов'язані з ними Облікові дані дозволяють Банку перевіряти походження Повідомлень, отриманих Банком.

More information regarding Authentication Methods for access to Services and/or connectivity channels may be accessed on the CitiDirect Login Help website. Customer may at any time select an available Authentication Method. During implementation of Services or connectivity channels, Bank may set-up a default Authentication Method, which Customer may change at any time to another available Authentication Method.

Більш детальну інформацію про Методи автентифікації для доступу до Послуг та/або каналів зв'язку можна отримати на вебсайті CitiDirect Допомога при реєстрації в системі. Клієнт може в будь-який час обрати доступний Метод автентифікації. Під час впровадження Послуг або каналів підключення Банк може встановити Метод автентифікації за замовчуванням, який Клієнт будь-коли може змінити на інший Метод автентифікації, доступний для нього.

The following Authentication Methods are available to access the services and/or connectivity channels:

Існують наступні Методи автентифікації, необхідні для здійснення доступу до Послуг та/або каналів підключення:

CitiDirect Authentication Methods Методи автентифікації CitiDirect	
Biometrics Біометрія	<p>A digital authentication method that utilizes a user's unique physical traits, (such as a fingerprint and facial recognition), built-in biometric technology on the user's mobile device, and cryptographic techniques to gain access to CitiDirect. Physical trait data is not transferred to the Bank when the user selects this authentication method.</p> <p><i>Цифровий метод автентифікації, який використовує унікальні фізичні характеристики користувача (наприклад, відбитки пальців та розпізнавання обличчя), вбудовану біометричну технологію на мобільному пристрої користувача та криптографічні методи для отримання доступу до CitiDirect. Якщо користувач обирає цей метод автентифікації, дані про його фізичні характеристики не передаються до Банку.</i></p>
Mobile Token (non-application based) Мобільний токен (не на основі застосунку)	<p>A digital non-application based mobile authentication method (e.g. Mobile Token (App-less)) that leverages cryptographic keys and biometric authentication (such as fingerprint and facial recognition) to link a user's mobile device to their CitiDirect account via the user's mobile browser. Physical trait data is not transferred to the Bank when the user selects this authentication method. This method facilitates multi-factor authentication by verifying the user's identity with their registered mobile device.</p> <p><i>Цифровий спосіб мобільної автентифікації не потребує використання застосунку (мобільний токен (без застосунку)). Зв'язок мобільного пристрою користувача з його обліковим записом CitiDirect відбувається через мобільний браузер користувача з використанням криптографічних ключів і біометричної автентифікації (розпізнавання відбитків пальців й обличчя). Коли користувач вибирає цей спосіб автентифікації, дані про фізичні ознаки не передаються до Банку. Цей спосіб полегшує багатофакторну автентифікацію завдяки перевірці особи користувача за допомогою його зареєстрованого мобільного пристрою.</i></p>
Challenge Response Token Токен метод «Запит-Відповідь»	<p>Either (i) a mobile application based soft token (e.g. MobilePASS) or (ii) a physical token (e.g. SafeWord Card, Vasco) which in each case is used to generate a dynamic password after authenticating with a PIN (e.g. 4-digit PIN). When accessing CitiDirect, the system generates a challenge and a response passcode is generated by the utilized token and entered into the system. This authentication method, when combined with a secure password results in multifactor authentication.</p> <p><i>(i) Програмний токен на основі мобільного додатку (наприклад, MobilePASS) або (ii) фізичний токен (наприклад, SafeWord Card, Vasco), який у кожному випадку використовується для генерації динамічного паролю після автентифікації за допомогою PIN-коду (наприклад, 4-значного PIN-коду). При вході в CitiDirect система генерує запит, тоді як пароль-відповідь генерується за допомогою токєну, що використовується, і вводиться в систему. Цей метод автентифікації в поєднанні з секретним паролем забезпечує багатофакторну автентифікацію.</i></p>
One-Time Password Token Токен з одноразовим паролем	<p>Either (i) a mobile application soft token (e.g. MobilePASS) or (ii) a physical token (e.g. SafeWord Card, Vasco) that is used to generate a dynamic password after authenticating with a PIN (e.g. 4-digit PIN). This dynamic password is entered into the system to gain access.</p> <p><i>(i) Програмний токен на основі мобільного додатку (наприклад, MobilePASS) або (ii) фізичний токен (наприклад, SafeWord Card, Vasco), який використовується для генерації динамічного паролю після автентифікації за допомогою PIN-коду (наприклад, 4-значного PIN-коду). Цей динамічний пароль вводиться в систему для отримання доступу.</i></p>

CitiDirect Authentication Methods Методи автентифікації CitiDirect	
Secure Password Секретний пароль	<p>A user enters his or her secure password to access the system. A secure password typically limits a user's capabilities on the system, for example, by only permitting that certain information be viewed by the user. This authentication method, when combined with a challenge response token results in multifactor authentication.</p> <p><i>Користувач вводить свій секретний пароль для доступу до системи. Секретний пароль зазвичай обмежує можливості користувача в системі, наприклад, дозволяючи користувачеві переглядати лише певну інформацію. Цей метод автентифікації в поєднанні з токеном методом "запит-відповідь" створює багатофакторну автентифікацію.</i></p>
SMS One-Time Code Одноразовий SMS-код	<p>A dynamic password delivered to users via SMS, after which the user enters the dynamic password and a secure password to gain access to the system.</p> <p><i>Динамічний пароль, який надсилається користувачам за допомогою SMS, після чого користувач вводить цей динамічний пароль та свій секретний пароль для отримання доступу до системи.</i></p>
Voice One-Time Code Голосовий одноразовий код	<p>A dynamic password delivered to users via an automated voice call, after which the user enters the dynamic password and a secure password to gain access to the system.</p> <p><i>Динамічний пароль, який надсилається користувачеві за допомогою автоматизованого голосового дзвінка, після чого користувач вводить цей динамічний пароль та свій секретний пароль для отримання доступу до системи.</i></p>
Digital Certificates Цифрові сертифікати	<p>A digital certificate is an electronic identification issued by an approved certificate authority for authentication and authorization. Digital certificates may be attributed to corporate legal entities ("Corporate Seals") or individuals ("Personal Certificates"). The Customer is responsible for properly verifying the identity of all users of Personal Certificates acting on behalf of the Customer in accordance with local law.</p> <p>The Bank and the Customer are required to use digital certificates provided by authorized persons, to ensure all Communications exchanged via a public internet connection or an otherwise unsecure internet connection are fully encrypted and protected.</p> <p><i>Цифровий сертифікат - це електронний ідентифікатор, виданий затвердженням центром сертифікації з метою автентифікації та авторизації. Цифрові сертифікати можуть бути призначені юридичним особам («Корпоративні печатки») або фізичним особам («Персональні сертифікати»). Клієнт несе відповідальність за належну перевірку особи всіх користувачів Персональних сертифікатів, які діють від імені Клієнта, відповідно до місцевого законодавства.</i></p> <p><i>Банк та Клієнт зобов'язані використовувати цифрові сертифікати, надані уповноваженими особами, для забезпечення повного шифрування та захисту всіх Комунікацій, якими обмінюються через публічне інтернет-з'єднання або іншим чином незахищене інтернет-з'єднання.</i></p>

CitiConnect for Files Authentication Methods Методи автентифікації CitiConnect для файлів	
Digital Certificates Цифрові сертифікати	<p>See description above.</p> <p><i>Див. опис вище.</i></p>

CitiConnect for Files Authentication Methods Методи автентифікації CitiConnect для файлів	
IP Address Whitelist When Using CitiConnect <i>Білий список IP-адрес при використанні CitiConnect</i>	<p>Certain Internet communications received by the Bank, for example, via a Virtual Private Network (VPN), may also rely on the parties exchanging information using pre-agreed Internet Protocol (IP) addresses. 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. Used in conjunction with Digital Certificate method above.</p> <p><i>Деякі Інтернет-повідомлення, отримані Банком, наприклад, через віртуальну приватну мережу (VPN), можуть також залежати від того, що сторони обмінюються інформацією, використовуючи попередньо узгоджені адреси Інтернет-протоколу (IP-адреси). Банк приймає тільки ті повідомлення, які надходять із зазначеної Клієнтом IP-адреси, і навпаки, і Банк передає тільки ті повідомлення, які надходять на зазначену Клієнтом IP-адресу, і навпаки. Використовується в поєднанні з методом Цифрового сертифікату, описаним вище.</i></p>
CitiConnect API Authentication Methods Методи автентифікації CitiConnect API	
Digital Certificates <i>Цифрові сертифікати</i>	<p>See description above.</p> <p><i>Див. опис вище.</i></p>
IP Address Whitelist When Using CitiConnect <i>Білий список IP-адрес при використанні CitiConnect</i>	<p>See description above.</p> <p><i>Див. опис вище.</i></p>
CitiConnect for SWIFT Authentication Methods Методи автентифікації CitiConnect для SWIFT	
Digital Certificates <i>Цифрові сертифікати</i>	<p>See description above. Can be used in conjunction with SWIFT Authentication method below.</p> <p><i>Дивіться опис вище. Може використовуватися разом з методом автентифікації SWIFT нижче.</i></p>

CitiConnect for SWIFT Authentication Methods Методи автентифікації CitiConnect для SWIFT	
SWIFT Authentication Автентифікація в системі SWIFT	<p>Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWIFT's Contractual Documentation (as 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 other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications.</p> <p>The Bank is not responsible for any errors or delays in the SWIFT system. The Customer is responsible for providing communications to the Bank in the format and type required and specified by SWIFT.</p> <p>Transmissions and Communications sent or received via SWIFT facilities are subject to SWIFT rules and regulations in effect, including membership rules. The Customer is responsible for being familiar with and conforming to SWIFT messaging standards.</p> <p><i>Повідомлення, що надсилаються між Банком та Клієнтом через мережу SWIFT, включаючи, але не обмежуючись, інформацію про рахунок, платіжні доручення та інструкції щодо внесення змін або скасування таких доручень, будуть автентифіковані з використанням процедур, визначених у Договірній документації SWIFT (зі змінами та доповненнями, що періодично вносяться до неї), яка включає, без обмежень, Загальні положення та умови, а також Опис фінансових послуг, або у порядку, визначеному в інших положеннях та умовах, що можуть бути встановлені SWIFT. Банк не зобов'язаний робити нічого, крім того, що передбачено процедурами SWIFT для встановлення відправника та автентичності цих Повідомлень.</i></p> <p><i>Банк не несе відповідальності за будь-які помилки або затримки в системі SWIFT. Клієнт несе відповідальність за надання Банку повідомлень у тому форматі та того типу, що вимагаються та визначені системою SWIFT.</i></p> <p><i>Перекази та Повідомлення, надіслані або отримані за допомогою засобів SWIFT, підпадають під дію чинних правил та положень SWIFT, включаючи правила членства. Клієнт несе відповідальність за ознайомлення зі стандартами обміну повідомленнями SWIFT та їх дотримання.</i></p>

SWIFT Authentication Method Метод автентифікації SWIFT	
SWIFT Authentication (Direct Connection for Financial Institutions) <i>Автентифікація SWIFT (пряме з'єднання для фінансових установ)</i>	<p>Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWIFT's Contractual Documentation (as 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 other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications.</p> <p>The Bank is not responsible for any errors or delays in the SWIFT system. The Customer is responsible for providing communications to the Bank in the format and type required and specified by SWIFT.</p> <p>Transmissions and Communications sent or received via SWIFT facilities are subject to SWIFT rules and regulations in effect, including membership rules. The Customer is responsible for being familiar with and conforming to SWIFT messaging standards.</p> <p><i>Повідомлення, що надсилаються між Банком та Клієнтом через мережу SWIFT, включаючи, але не обмежуючись, інформацію про рахунок, платіжні доручення та інструкції щодо внесення змін або скасування таких доручень, будуть автентифіковані з використанням процедур, визначених у Договірній документації SWIFT (зі змінами та доповненнями, що періодично вносяться до неї), яка включає, без обмежень, Загальні положення та умови, а також Опис фінансових послуг, або у порядку, визначеному в інших положеннях та умовах, що можуть бути встановлені SWIFT. Банк не зобов'язаний робити нічого, крім того, що передбачено процедурами SWIFT для встановлення відправника та автентичності цих Повідомлень.</i></p> <p><i>Банк не несе відповідальності за будь-які помилки або затримки в системі SWIFT. Клієнт несе відповідальність за надання Банку повідомлень у тому форматі та того типу, що вимагаються та визначені системою SWIFT.</i></p> <p><i>Перекази та Повідомлення, надіслані або отримані за допомогою засобів SWIFT, підпадають під дію чинних правил та положень SWIFT, включаючи правила членства. Клієнт несе відповідальність за ознайомлення зі стандартами обміну повідомленнями SWIFT та їх дотримання.</i></p>
Digital/Electronic Signature Authentication Methods for Electronic Document Submission Методи автентифікації за допомоги цифрового/електронного підпису для електронного подання документів	
Digital Signature <i>Цифровий підпис</i>	<p>A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document.</p> <p><i>Тип електронного підпису, який використовує цифрові сертифікати для підтвердження автентичності та цілісності підпису, повідомлення, програмного забезпечення або цифрового документа.</i></p>

Digital/Electronic Signature Authentication Methods for Electronic Document Submission Методи автентифікації за допомоги цифрового/електронного підпису для електронного подання документів

Electronic Signature Електронний підпис	<p>An electronic symbol attached to a contract or other record, unique to and used by a person with an intent to sign. Electronic signatures can be established in the form of words, letters, numerals, symbols, click of a button on a website, upload of facsimile or scan of a physical signature, signing on a touchscreen, or agreeing to any terms and conditions by electronic means. Created under the sole control of the person using it, it is logically attached to or associated with a data message capable of identifying the person who consents to the data message and certifying the person's consent. Such Electronic Signature would be submitted to the Bank through the Bank's electronic channels and in compliance with the associated Authentication Methods described above.</p> <p><i>Електронний символ, що додається до контракту або іншого запису, унікальний для особи, яка має намір його підписати. Електронний підпис може бути створений у вигляді слів, літер, цифр, символів, натискання кнопки на вебсайті, завантаження факсиміле або сканування фізичного підпису, підпису на сенсорному екрані або згоди з будь-якими умовами та положеннями за допомогою електронних засобів. Створений під виключним контролем особи, яка його використовує, він логічно приєднується до повідомлення даних або асоціюється з ним, що дозволяє ідентифікувати особу, яка дає згоду на повідомлення даних, і засвідчує її згоду. Такий Електронний підпис подається до Банку через електронні канали Банку та з дотриманням відповідних Методів автентифікації, описаних вище.</i></p>
--	---

Manual Initiated Funds Transfer (MIFT) Authentication Method Метод автентифікації переказу коштів, ініційованого вручну (MIFT)

MIFT Authentication Автентифікація MIFT	<p>Manually Initiated Funds Transfer (MIFT), including amendments, recalls, or cancellations of previous manual instructions, may be made by fax or letter or upload to CitiDirect. Not all forms are supported in all countries. Initiators are persons designated by the Customer who are authorized to initiate transactions in accordance with restrictions, if any, are identified by the Customer. Confirmers are person designated by the Customer that Bank may call back, at its discretion, for confirmation of manually initiated instructions for funds transfers.</p> <p>In certain countries, mobile telephone numbers are not accepted as call back numbers. Further details are provided in the applicable Country Cash Management User Guide, Global Manual Transaction Authorization or Universal Nomination Form. MIFT is to be used by the Customer as a contingency method to communication instructions to the Bank.</p> <p><i>Автентифікація переказу коштів, ініційованого вручну (MIFT), включаючи зміни, відкликання або скасування попередніх інструкцій, може бути здійснена факсом, листом або завантажена в CitiDirect. Не всі форми підтримуються в усіх країнах. Ініціатори - особи, визначені Клієнтом, які уповноважені ініціювати операції відповідно до обмежень, якщо такі визначені Клієнтом. Підтверджувачі – це визначені Клієнтом особи, яким Банк може передзвонити на власний розсуд для підтвердження інструкцій з переказу коштів ініційованих вручну.</i></p> <p><i>У деяких країнах номери мобільних телефонів не приймаються як номери для зворотного дзвінка. Більш детальну інформацію наведено у відповідному Посібнику користувача з управління грошовими коштами в країні, Глобальній інструкції з авторизації транзакцій вручну або Універсальній формі номінації. Клієнт повинен використовувати MIFT як резервний метод передачі інструкцій Банку.</i></p>
--	--

Mail, Fax, Email and Messenger Authentication Methods Методи автентифікації за допомогою пошти, факсу, електронної пошти та месенджерів	
Seal Image Verification Перевірка зображення печатки	Correspondence received by the Bank via fax, mail, email or messenger, excluding MIFT requests, are verified and collated with due care based on the seal image contained in the Customer's authority document or similar document provided to the Bank. <i>За винятком запитів MIFT, кореспонденція, отримана Банком факсом, поштою, електронною поштою або месенджером, перевіряється та зіставляється з належною ретельністю на основі зображення печатки, що міститься в документі про повноваження Клієнта або аналогічному документі, наданому Банку.</i>
Signature Verification Перевірка підпису	Correspondence received by the Bank via fax, mail, email or messenger, excluding MIFT requests, are signature verified based on the information contained in the Customer's authority document or similar document provided to the Bank. <i>За винятком запитів MIFT, кореспонденція, отримана Банком факсом, поштою, електронною поштою або месенджером, перевіряється на підставі інформації, що міститься в наданому Банку документі про повноваження Клієнта або аналогічному документі.</i>
Secure PDF Захищений документ у форматі PDF	Encrypted emails are delivered to a regular mailbox as PDF documents that are opened by entering a private password. Both the message and body and any attached files are encrypted. A private password can be set up upon receipt of the first secure email received. <i>Зашифровані електронні листи в форматі PDF доставляються на звичайну поштову скриньку у вигляді документів у форматі PDF, які відкриваються шляхом введення особистого пароля. Шифруються як повідомлення, так і тіло листа, а також будь-які прикріплені файли. Особистий пароль можна встановити після отримання першого захищеного електронного листа.</i>
MTLS MTLS	Mandatory Transport Layer Security (MTLS) creates what would be a secure, private email connection between the Bank and the Customer. Emails transmitted using this channel are sent over the internet though encrypted TLS tunnel created by the connection. <i>Обов'язковий захист на рівні транспортування (Mandatory Transport Layer Security, MTLS) створює так зване захищене, приватне з'єднання електронної пошти між банком і клієнтом. Електронні листи, що передаються цим каналом, надсилаються через Інтернет через зашифрований TLS-тунель, створений під час з'єднання.</i>

Phone Authentication Methods Методи телефонної автентифікації	
PIN PIN-код	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. <i>Клієнтам, які зв'язуються з Банком по телефону, пропонується ввести PIN-код для підтвердження авторизованого доступу.</i>

Phone Authentication Methods Методи телефонної автентифікації	
Verification Questions Верифікаційні питання	<p>Customers contacting the Bank via phone are prompted by the Bank's service representatives to provide correct verbal responses to verification questions in order to validate authorized access.</p> <p>Клієнтам Банку, які звертаються по телефону, представники по роботі з клієнтами пропонують надати коректні усні відповіді на верифікаційні питання з метою підтвердження авторизованого доступу.</p>

The availability of Authentication Methods described above varies based on local markets.

Доступність описаних вище методів автентифікації залежить від місцевих ринків.

3. Customer Responsibilities Обов'язки Клієнта

- 3.1 Identifying Authorized Users: Customer is responsible for identifying: (i) all individuals acting on the authenticate the Customer's Account(s) on behalf of the Customer at an entity level for all Services and connectivity channels, and (ii) each person acting on behalf of the Customer being duly authorized by the Customer to act on the Customer's Account.

Ідентифікація Авторизованих користувачів: Клієнт несе відповідальність за ідентифікацію: (i) усіх фізичних осіб, які діють від імені Клієнта на рівні юридичної особи для всіх Послуг та каналів зв'язку, та (ii) кожну особу, яка діє від імені Клієнта, належним чином уповноважену Клієнтом діяти з Акаунтом Клієнта.

- 3.2 Customer is responsible for assigning and monitoring any transaction limits assigned to the Customer and/or its users and ensuring that these limits (a) do not exceed the limits as required by the Customer's internal policies and other authority and constitutive documents such as Customer's Board of Director resolutions, Bank Mandates, Power Of Attorney, or equivalent document, and (b) are properly reflected on all connectivity channels and user entitlements.

Клієнт несе відповідальність за встановлення та моніторинг будь-яких лімітів на транзакції, призначених Клієнту та/або його користувачам, а також за забезпечення того, щоб ці ліміти (a) не перевищували лімітів, передбачених внутрішніми політиками та іншими повноваженнями та установчими документами Клієнта, такими як рішення Ради директорів Клієнта, банківські доручення, довіреності або еквівалентні документи, та (b) були належним чином відображені на всіх каналах підключення та правах користувачів.

- 3.3 Certain jurisdictions may require individuals (and their corresponding Credentials) to be identified by the Bank in accordance with applicable AML legislation requirements before granting access to perform certain functions. Please contact your Customer Service Representative or visit the CitiDirect website for further information.

Деякі юрисдикції можуть вимагати, щоб Банк ідентифікував фізичних осіб (та їхні відповідні Облікові дані) відповідно до вимог чинного законодавства у сфері протидії відмиванню коштів, перш ніж надавати доступ до виконання певних функцій. Для отримання додаткової інформації, будь ласка, зверніться до свого представника по роботі з клієнтами або відвідайте вебсайт CitiDirect.

3.4 Safeguarding of Authentication Methods *Захист методів автентифікації*

The Customer is responsible for safeguarding the Authentication Methods and Credentials with the highest standard of care and diligence, and ensuring that access to and distribution of the Credentials are limited only to persons that have been authorized by the Customer.

Communications sent by a third party: Where the Customer is using a Credential to identify and authenticate their Communications as originating from them as a legal entity, the Customer is responsible for exercising full control over the use of such Credentials when sending Communications to the Bank, including where such Communications are sent by applications and/or systems that are managed by a third party on behalf of the Customer. In all circumstances the Bank will (a) deem any Communication it receives through an electronic connectivity channel, that has been received by the Bank in compliance with these Security Procedures duly authenticated as originating from the Customer, as a Communication instructed by the Customer and (b) may act upon any Communication that it receives on behalf of the Customer in compliance with these Security Procedures.

Клієнт несе відповідальність за захист Методів автентифікації та Облікових даних з найвищим рівнем обережності та старанності, а також за забезпечення того, щоб доступ до Облікових даних та їх розповсюдження обмежувався лише особами, які були уповноважені Клієнтом.

Повідомлення, надіслані третьою стороною: Якщо Клієнт використовує Облікові дані для ідентифікації та автентифікації своїх Повідомлень як таких, що походять від нього як юридичної особи, Клієнт несе відповідальність за здійснення повного контролю за використанням таких Облікових даних при надсиланні Повідомлень Банку, в тому числі, якщо такі Повідомлення надсилаються за допомогою додатків та/або систем, які управляються третьою особою від імені Клієнта. За будь-яких обставин Банк (а) буде вважати будь-яке Повідомлення, отримане ним через електронний канал зв'язку, яке було отримано Банком відповідно до цих Процедур безпеки, належним чином засвідчене як таке, що походить від Клієнта, як Повідомлення за дорученням Клієнта, та (б) може діяти на підставі будь-якого Повідомлення, отриманого ним від імені Клієнта, відповідно до цих Процедур безпеки.

4. Data Integrity and Secured Communications *Цілісність даних та захищені комунікації*

- 4.1 The Customer will be transmitting data to and otherwise exchanging Communications with the Bank, utilizing the internet, mail, email and/or fax which the Customer understands are not (i) necessarily secure communications and delivery systems, and (ii) under the Bank's control. The Customer further understands that if Customer's users are entitled to access Open Banking and/or similar third-party platforms outside of the Citi systems, Customer data could be transmitted over such third-party platforms which are not under the Bank's control.

Клієнт передаватиме дані до Банку та в інший спосіб обмінюватиметься повідомленнями з ним, використовуючи Інтернет, пошту, зокрема електронну пошту, і/або факс, які, на думку Клієнта, (i) не є гарантовано безпечними системами зв'язку та доставлення, (ii) не перебувають під контролем Банку. Клієнт також розуміє, що якщо користувачі Клієнта мають право доступу до Відкритого банкінгу та/чи подібних сторонніх платформ поза системами Citi, дані Клієнта можуть передаватися через такі сторонні платформи, які не перебувають під контролем Банку.

- 4.2 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 electronic transit.

Банк використовує провідні в галузі методи шифрування (за визначенням Банку), які допомагають забезпечити конфіденційність інформації та її незмінність під час електронного передавання.

- 4.3 If the Customer suspects or becomes aware of a technical failure or any improper or potentially fraudulent access to or use of the Bank's Services or connectivity channels or 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 or potentially fraudulent 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.

Якщо Клієнт підозрює або дізнається про технічний збій або будь-який неналежний чи потенційно шахрайський доступ або використання Послуг Банку або каналів зв'язку чи Методів автентифікації будь-якою особою (незалежно від того, чи є вона уповноваженою особою чи ні), Клієнт зобов'язаний негайно повідомити Банк про таку подію. У випадку неналежного або потенційно шахрайського доступу або використання уповноваженою особою, Клієнт повинен негайно вжити заходів для припинення доступу та використання такою уповноваженою особою Послуг або каналів зв'язку Банку.

- 4.4 If the Customer utilizes file formatting or 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 the Bank, the Customer will use such software solely for the purpose for which it has been installed.

Якщо Клієнт використовує програмне забезпечення для форматування файлів або шифрування (надане Банком або третьою особою) для підтримки форматування та розпізнавання даних та інструкцій Клієнта, а також для здійснення комунікацій з Банком, Клієнт зобов'язується використовувати таке програмне забезпечення виключно з тією метою, для якої воно було встановлене.

- 4.5 The Customer accepts that the Bank may suspend or deny users' access to Services requiring the use of Credentials (i) in case of suspicion of unauthorized or fraudulent use of the Credentials and/or (ii) to safeguard the Services or Credentials.

Клієнт погоджується з тим, що Банк має право призупинити або відмовити користувачам у доступі до Послуг, що вимагають використання Облікових даних (i) у разі підозри в несанкціонованому або шахрайському використанні Облікових даних та/або (ii) з метою забезпечення безпеки Послуг або Облікових даних.

5. Security Manager and Related Functions Менеджер з безпеки та пов'язані з ним функції

For applications accessible in CitiDirect and CitiConnect (with the exception of Personal Certificates discussed below), the Bank requires the Customer to establish a "Security Manager" function. Security Managers are responsible for:

Для додатків, доступних у CitiDirect та CitiConnect (за винятком Персональних сертифікатів, про які йдеться нижче), Банк вимагає, щоб Клієнт створив функцію «Менеджер з безпеки». Менеджери з безпеки несуть відповідальність за наступне:

- 5.1 Establishing and maintaining the access and entitlements of users (including Security Managers themselves) including activities such as: (a) creating, deleting or modifying user Profiles (including Security Manager Profiles) and entitlement rights (Note that user name must align with supporting identification documents); (b) building access profiles that define the functions and data available to individual users; (c) enabling and disabling user log-on credentials; and (d) assigning transaction limits (Note these limits are not monitored or validated by the Bank and Customer should monitor these limits to ensure they are in compliance with the Customer's internal policies and requirements, including but not limited to, those established by the Customer's Board of Directors or equivalent);

Встановлення та підтримання доступу та прав користувачів (включаючи самих Менеджерів з безпеки), включаючи такі види діяльності, як (a) створення, видалення або зміну профілів користувачів

(включаючи профілі менеджерів з безпеки) та прав доступу (зверніть увагу, що ім'я користувача повинно відповідати підтверджуючим документам, що посвідчують особу); (b) створення профілів доступу, які визначають функції та дані, доступні окремим користувачам; (c) ввімкнення та вимкнення облікових даних для входу в систему користувачів; та (d) встановлення лімітів на операції (Зверніть увагу, що ці ліміти не контролюються та не підтверджуються Банком, і Клієнт повинен контролювати ці ліміти, щоб переконатися, що вони відповідають внутрішнім політикам та вимогам Клієнта, включаючи, але не обмежуючись, встановленими Радою директорів Клієнта або еквівалентними документами);

- 5.2 Creating and modifying entries in Customer maintained libraries (such as preformatted payments and beneficiary libraries) and authorizing other users to do the same;

Створювати та змінювати записи в бібліотеках, що підтримуються Клієнтом (наприклад, попередньо відформатовані платежі та бібліотеки одержувачів), а також надавати іншим користувачам повноваження робити те саме;

- 5.3 Modifying payment authorization flows;

Модифікація потоків авторизації платежів;

- 5.4 Allocating dynamic password credentials or other system access credentials or passwords to the Customer's users;

Надання користувачам Клієнта облікових даних динамічного пароля або інших облікових даних чи паролів доступу до системи;

- 5.5 Notifying the Bank, if there is any reason to suspect that security has been compromised; and

Повідомлення Банку, якщо є підстави підозрювати, що безпека була порушена; та

- 5.6 Managing and procuring digital certificates and authorizing other users to do the same.

Управління та придбання цифрових сертифікатів та надання повноважень іншим користувачам робити те саме.

Please note: Security Manager roles and responsibilities may vary or not be applicable in certain markets due to regulatory requirements and/or operational capabilities. In such markets, the Bank may require additional documentation and other information from the Customer to perform Security Manager functions on behalf of the Customer.

Зверніть увагу: Функції та обов'язки менеджера з безпеки можуть відрізнятися або не застосовуватися на певних ринках через регуляторні вимоги та/або операційні можливості. На таких ринках Банк може вимагати від Клієнта додаткову документацію та іншу інформацію для виконання функцій Менеджера з безпеки від імені Клієнта.

6. Use of CitiDirect and CitiConnect by Security Managers **Використання Менеджерами з безпеки CitiDirect та CitiConnect**

The Bank requires two (2) 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 communications. Any such communications, when authorized by two Security Managers, will be accepted and acted on by the Bank and deemed to be given by the Customer. The Bank recommends the designation of at least three Security Managers to ensure adequate backup. The Customer shall designate Customer's 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.

Банк вимагає, щоб введення та авторизація інструкцій здійснювалися 2 (двома) окремими фізичними особами; отже, необхідно мати щонайменше двох Менеджерів з безпеки. Будь-які два менеджери з безпеки, діючи спільно, можуть надавати інструкції та/або підтвердження через канали зв'язку стосовно будь-якої функції менеджера з безпеки або у зв'язку із забезпеченням комунікацій. Будь-які такі повідомлення, санкціоновані двома Менеджерами з безпеки, приймаються та виконуються Банком і вважаються такими, що надані Клієнтом. Банк рекомендує призначити щонайменше трьох Менеджерів з безпеки для забезпечення належної заміни. Клієнт призначає Менеджерів з безпеки в Формі встановлення доступу до каналів TTS. Менеджер з безпеки Клієнта може також діяти як Менеджер з безпеки третьої сторони (наприклад, афілійованої особи Клієнта) та здійснювати всі пов'язані з цим права (включаючи призначення користувачів для Рахунку(ів) цієї третьої сторони) без будь-якого додаткового призначення, якщо ця третя сторона оформлює форму Універсального дозволу на доступ (або іншу прийнятну для Банку форму дозволу), що надає Клієнту доступ до її Рахунку(ів). Це стосується лише тих Рахунків, на які поширюється відповідний дозвіл.

7. Use of CitiDirect by Security Officers (For Personal Certificates only) ***Використання CitiDirect співробітниками служби безпеки (лише для персональних сертифікатів)***

The Bank requires two (2) separate individuals to manage digital certificates attributed to individuals ("Personal Certificates"). Therefore, two Security Officers are required to assign and remove Personal Certificates to users, for the purpose of authenticating and authorizing Communications on the connectivity channels. The Bank recommends the designation of at least three Security Officers to ensure adequate backup. Any Communications authorized by Personal Certificates will be accepted and acted on by the Bank and deemed to be given by the Customer.

Банк вимагає, щоб управління цифровими сертифікатами, що належать фізичним особам («Персональні сертифікати»), здійснювали 2 (дві) окремі особи. Таким чином, два співробітники служби безпеки повинні призначати та відкликати персональні сертифікати для користувачам з метою автентифікації та авторизації Комунікацій на каналах зв'язку. Банк рекомендує призначати щонайменше трьох співробітників служби безпеки для забезпечення належного резервного копіювання. Будь-які Повідомлення, авторизовані Персональними сертифікатами, приймаються та виконуються Банком і вважаються такими, що надані Клієнтом.