citi handlowy

Security Procedures
Procedury Bezpieczeństwa

1. Introduction
Wprowadzenie

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).

Niniejsze „Procedury Bezpieczeństwa", zgodnie z informacjami w punkcie „Komunikacja" Ogólnych Warunków Prowadzenia Rachunków i Świadczenia Usług („Ogólne Warunki") (lub innymi mającymi zastosowanie warunkami prowadzenia rachunków), opracowano na potrzeby procesu uwierzytelniania logowania Klienta w kanałach dostępu Banku oraz w celu weryfikacji pochodzenia Komunikatów przesyłanych pomiędzy Bankiem a Klientem w związku z poniższymi Usługami lub kanałami dostępu (ich dostępność może być różna na poszczególnych rynkach lokalnych).

- CitiDirect BE® (including WorldLink®)
  CitiDirect BE® (w tym WorldLink®)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  SWIFT (ang. Society for Worldwide Interbank Financial Telecommunication)
- Manual Initiated Funds Transfer ("MIFT")
  MIFT (ang. Manually Initiated Funds Transfer) dyspozycja płatnicza w formie papierowej
- Interactive Voice Response ("IVR")
  IVR (ang. Interactive Voice Response) Automatyczny System Informacji Głosowej
- Email/Fax/Mail/Messenger/Phone with the Bank
  poczta elektroniczna/faks/poczta/komunikator/telefon z Bankiem
- Other local electronic connectivity channels
  inne lokalne elektroniczne kanały dostępu

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 BE. 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:

Niniejsze Procedury Bezpieczeństwa należy czytać łącznie z Ogólnymi Warunkami. Mogą być uaktualniane i przekazane Klientowi drogą elektroniczną lub inną, w tym w szczególności poprzez informację o aktualizacji Procedur Bezpieczeństwa udostępnioną w CitiDirect BE. O ile prawo nie stanowi inaczej, dalsze korzystanie przez Klienta z którychkolwiek ze wskazanych wyżej Usług lub kanałów dostępu po poinformowaniu Klienta o aktualizacji Procedur Bezpieczeństwa stanowi akceptację przez Klienta takich uaktualnionych Procedur Bezpieczeństwa. Niniejsze Procedury Bezpieczeństwa obejmują:

A. Authentication Methods
Metody Uwierzytelniania

B. Customer Responsibilities
Zakres obowiązków Klienta

C. Data Integrity and Secured Communications
Integralność Danych i Bezpieczna Komunikacja

D. Security Manager and Related Functions
Administrator Systemu i Powiązane Funkcje

2. Authentication Methods
Metody Uwierzytelniania

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.

Procedury Bezpieczeństwa obejmują bezpieczne metody uwierzytelniania („Metody Uwierzytelniania") stosowane w celu jednoznacznej identyfikacji i weryfikacji uprawnień Klienta i/lub któregokolwiek z użytkowników upoważnionych przez Klienta, zwykle z użyciem jednego lub połączenia mechanizmów takich jak ID użytkownika/hasło użytkownika, certyfikaty cyfrowe, biometria, tokeny (dostarczane w formie sprzętowej lub aplikacyjnej), weryfikacja pieczęci/podpisu i/lub urządzenia powiązane z Metodami Uwierzytelniania (określane łącznie jako „Narzędzia Uwierzytelniające"). Metody Uwierzytelniania i powiązane Narzędzia Uwierzytelniające umożliwiają Bankowi weryfikowanie źródła pochodzenia Komunikatów otrzymanych przez Bank.

More information regarding Authentication Methods for access to Services and/or connectivity channels may be accessed on the CitiDirect BE 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.

Więcej informacji o Metodach Uwierzytelniania dostępu do Usług i/lub kanałów dostępu można znaleźć w sekcji „Potrzebujesz pomocy?" na stronie logowania CitiDirect BE. Klient może w każdej chwili wybrać dostępną Metodę Uwierzytelniania. W trakcie wdrażania Usług lub kanałów dostępu Bank może skonfigurować domyślną Metodę Uwierzytelniania, którą Klient może zmienić w każdej chwili na inną dostępną Metodę Uwierzytelniania.

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

Następujące Metody Uwierzytelniania dostępne są podczas logowania do Usług i/lub kanałów dostępu:

CitiDirect BE Authentication Methods *Metody Uwierzytelniania w CitiDirect BE*	
Biometrics *Biometria*	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 BE. Physical trait data is not transferred to the Bank when the user selects this authentication method. *Cyfrowa metoda uwierzytelniania wykorzystująca niepowtarzalne cechy fizyczne użytkownika (takie jak odcisk palca i rozpoznawanie twarzy), technologię biometryczną wbudowaną w urządzeniu mobilnym użytkownika oraz techniki kryptograficzne w celu uzyskania dostępu do CitiDirect BE. Dane zawierające cechy fizyczne nie są przekazywane do Banku, gdy użytkownik wybierze tę Metodę Uwierzytelniania.*

Challenge Response Token *Token: zapytanie - odpowiedź*	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 BE, 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. *Albo (i) aplikacja mobilna, soft token (np. MobilePASS), albo (ii) token fizyczny (np. SafeWord Card, Vasco), każdorazowo stosowany w celu wygenerowania dynamicznego hasła po wcześniejszym uwierzytelnieniu np. 4 - cyfrowym numerem PIN. Podczas logowania do CitiDirect BE system generuje zapytanie, a wygenerowane tokenem hasło jest wprowadzane do systemu. Ta metoda uwierzytelniania, w połączeniu z bezpiecznym hasłem, składa się na uwierzytelnianie wielostopniowe.*
One-Time Password Token *Token: jednorazowe hasło*	Either (i) a mobile application based 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. *Albo (i) aplikacja mobilna, soft token (np. MobilePASS), albo (ii) token fizyczny (np. SafeWord Card, Vasco), każdorazowo stosowany w celu wygenerowania dynamicznego hasła po wcześniejszym uwierzytelnieniu np. 4 - cyfrowym numerem PIN. To dynamiczne hasło jest wprowadzane do systemu w celu uzyskania dostępu.*
Secure Password *Bezpieczne Hasło*	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. *Użytkownik wprowadza swoje bezpieczne hasło, by uzyskać dostęp do systemu. Bezpieczne hasło zwykle ogranicza zakres funkcjonalności dostępnych dla użytkownika w systemie, np. pozwala użytkownikowi jedynie przeglądać pewne informacje. Ta metoda uwierzytelniania, w połączeniu z Tokenem: zapytanie - odpowiedź, składa się na uwierzytelnianie wielostopniowe.*
SMS One-Time Code *Jednorazowy kod SMS*	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. *Dynamicznie generowane i bezpieczne hasło dostarczane użytkownikowi poprzez SMS, które użytkownik wprowadza na stronie logowania, by uzyskać dostęp do systemu.*
Voice One-Time Code *Jednorazowy kod otrzymany głosowo przez telefon*	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. *Hasło jest podawane użytkownikowi telefonicznie przez automat głosowy, po czym użytkownik wprowadza je do systemu podczas logowania.*

Digital Certificates *Certyfikaty cyfrowe*	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. *Certyfikat cyfrowy jest to elektroniczny identyfikator wystawiony przez zatwierdzony podmiot certyfikujący na potrzeby uwierzytelniania i autoryzacji. Certyfikaty cyfrowe mogą być przypisane do osób prawnych („Pieczęci Firmowe") lub osób fizycznych („Certyfikaty Osobiste"). Klient jest odpowiedzialny za prawidłową weryfikację wszystkich użytkowników Certyfikatów Osobistych zgodnie z lokalnym prawem.* 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. *Bank i Klient muszą stosować certyfikaty cyfrowe dostarczone przez osoby upoważnione, aby zapewnić, że wszystkie Komunikaty wymieniane poprzez publiczne łącza internetowe lub z innych względów niebezpieczne łącza internetowe są w pełni zaszyfrowane i chronione.*

CitiConnect for Files Authentication Methods *CitiConnect dla Metod Uwierzytelniania Plików*	
Digital Certificates *Certyfikaty cyfrowe*	See description above. *Zobacz opis powyżej.*
IP Address Whitelist When Using CitiConnect *Lista Zaufanych Adresów IP (Whitelist) w trakcie korzystania z CitiConnect*	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. *Niektóre komunikaty internetowe otrzymywane przez Bank, np. poprzez Wirtualną Sieć Prywatną (Virtual Private Network - VPN), mogą również polegać na podmiotach wymieniających informacje z użyciem adresów internetowych (IP). Bank przyjmuje Komunikację wyłącznie pochodzącą ze wskazanego adresu IP Klienta, i odwrotnie, i wysyła tylko Komunikację na wskazany adres IP Klienta, i odwrotnie. Używane w połączeniu z opisaną wyżej metodą opartą o Certyfikaty Cyfrowe.*

CitiConnect API Authentication Methods *Metody Uwierzytelniania CitiConnect API*	
Digital Certificates *Certyfikaty cyfrowe*	See description above. *Zobacz opis powyżej.*
IP Address Whitelist When Using CitiConnect *Lista Zaufanych Adresów IP (Whitelist) w trakcie korzystania z CitiConnect*	See description above. *Zobacz opis powyżej.*

CitiConnect for SWIFT Authentication Methods *Metody Uwierzytelniania CitiConnect for SWIFT*	
Digital Certificates *Certyfikaty cyfrowe*	See description above. Can be used in conjunction with SWIFT Authentication method below. *Zobacz opis powyżej. Mogą być stosowane w połączeniu z Metodą Uwierzytelniania SWIFT, opisaną poniżej.*
SWIFT Authentication *SWIFT Uwierzytelnianie*	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. *Komunikaty przesyłane pomiędzy Bankiem a Klientem przez sieć SWIFT, w tym między innymi informacje o rachunku, zlecenia płatnicze oraz dyspozycje anulowania takich zleceń, będą uwierzytelniane z zastosowaniem procedur określonych w Dokumentacji Umownej organizacji SWIFT (z późniejszymi zmianami lub uzupełnieniami), która zawiera między innymi jej Ogólne Warunki oraz Opis Usług FIN albo zgodnie z innymi warunkami, które mogą zostać określone przez SWIFT. Bank nie jest zobowiązany do podejmowania jakichkolwiek czynności poza tymi, które określono w procedurach SWIFT, w celu ustalenia tożsamości nadawcy oraz autentyczności tych Komunikatów.* 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. *Bank nie odpowiada za jakiekolwiek błędy i opóźnienia w systemie SWIFT. Klient jest odpowiedzialny za przekazywanie Komunikatów do Banku zgodnie z wymogami SWIFT dotyczącymi formatu i rodzaju.* 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. *Transmisje i Komunikaty wysłane lub otrzymane poprzez systemy SWIFT podlegają obowiązującym zasadom i regulacjom SWIFT, w tym zasadom członkostwa. Klient ma obowiązek znać standardy dotyczące komunikatów SWIFT i przestrzegać ich.*

SWIFT Authentication Method *Metody Uwierzytelniania SWIFT*	
SWIFT Authentication (Direct Connection for Financial Institutions) *SWIFT Uwierzytelnianie (Bezpośrednie Połączenie dla Instytucji Finansowych)*	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. *Komunikaty przesyłane pomiędzy Bankiem a Klientem przez sieć SWIFT, w tym między innymi informacje o rachunku, zlecenia płatnicze oraz dyspozycje anulowania takich zleceń, będą uwierzytelniane z zastosowaniem procedur określonych w Dokumentacji Umownej organizacji SWIFT (z późniejszymi zmianami lub uzupełnieniami), która zawiera między innymi jej Ogólne Warunki oraz Opis Usług FIN albo zgodnie z innymi warunkami, które mogą zostać określone przez SWIFT. Bank nie jest zobowiązany do podejmowania jakichkolwiek czynności poza tymi, które określono w procedurach SWIFT, w celu ustalenia tożsamości nadawcy oraz autentyczności tych Komunikatów.* 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. *Bank nie odpowiada za jakiekolwiek błędy i opóźnienia w systemie SWIFT. Klient jest odpowiedzialny za przekazywanie Komunikatów do Banku zgodnie z wymogami SWIFT dotyczącymi formatu i rodzaju.* 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. *Transmisje i Komunikaty wysłane lub otrzymane poprzez systemy SWIFT podlegają obowiązującym zasadom i regulacjom SWIFT, w tym zasadom członkostwa. Klient ma obowiązek znać standardy dotyczące komunikatów SWIFT i przestrzegać ich.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission *Metody Uwierzytelniania podpisem cyfrowym/elektronicznym przy składaniu dokumentów elektronicznych*	
Digital Signature *Podpis cyfrowy*	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. *Rodzaj podpisu elektronicznego, który wykorzystuje certyfikaty cyfrowe do potwierdzenia autentyczności i integralności podpisu, komunikatu, programu lub dokumentu cyfrowego.*

Electronic Signature *Podpis elektroniczny*	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. *Elektroniczny symbol dołączony do umowy lub innego rekordu, niepowtarzalny dla osoby i używany przez nią z zamiarem złożenia podpisu. Podpisy elektroniczne można tworzyć w formie słów, liter, cyfr, symboli, kliknięcia przycisku na stronie internetowej, wprowadzenia faksu lub skanu fizycznego podpisu, złożenia podpisu na ekranie dotykowym lub zatwierdzenia warunków za pomocą środków elektronicznych. Utworzony pod wyłączną kontrolą swojego użytkownika, podpis elektroniczny jest powiązany logicznie z komunikatem zawierającym dane mogące zidentyfikować osobę, która wyraziła zgodę na ten komunikat, i poświadczyć zgodę tej osoby. Taki podpis elektroniczny zostałby złożony w Banku poprzez kanały elektroniczne należące do Banku oraz zgodnie z powiązanymi Metodami Uwierzytelniania opisanymi powyżej.*

Manual Initiated Funds Transfer (MIFT) Authentication Method *Metoda Uwierzytelniania dyspozycji płatniczej w formie papierowej („MIFT")*	
MIFT Authentication *Uwierzytelnianie MIFT*	Manually Initiated Funds Transfer (MIFT), including amendments, recalls, or cancelations 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. *Dyspozycja płatnicza w formie papierowej MIFT, w tym zmiany, odwołania lub anulowania poprzednich dyspozycji płatniczych w formie papierowej, można realizować faksem lub pisemnie albo poprzez wprowadzenie do CitiDirect BE. Nie wszystkie formy są obsługiwane we wszystkich krajach. Osobami upoważnionymi do podpisywania dyspozycji płatniczych składanych na formularzach papierowych są osoby wyznaczone przez Klienta w stosownym upoważnieniu, które są upoważnione do podpisywania dyspozycji płatniczych zgodnie z ograniczeniami, jeśli występują, określonymi przez Klienta. Osobami upoważnionymi do potwierdzania dyspozycji płatniczych są osoby wyznaczone przez Klienta, do których Bank może oddzwonić według własnego uznania w celu potwierdzenia dyspozycji płatniczej.* 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 communicating instructions to the Bank. *W niektórych krajach numery telefonów komórkowych nie są akceptowane jako numery do kontaktu w celu potwierdzania dyspozycji płatniczych. Dalsze szczegóły podano we właściwym Podręczniku dotyczącym usług świadczonych przez Bank i w Upoważnieniu do Potwierdzania Dyspozycji Płatniczych w Formie Papierowej lub Formularzu Uniwersalnej Nominacji. Klient będzie stosował MIFT jako awaryjną metodę przekazywania dyspozycji Bankowi.*

Mail, Fax, Email and Messenger Authentication Methods *Metody Uwierzytelniania pocztą, faksem, pocztą elektroniczną i komunikatorem*	
Seal Image Verification *Weryfikacja Obrazem Pieczęci*	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. *Korespondencja otrzymana przez Bank faksem, pocztą, pocztą elektroniczną lub komunikatorem, z wyłączeniem wniosków MIFT, jest weryfikowana i segregowana z należytą starannością na podstawie obrazu pieczęci zawartego w dokumencie upoważnienia otrzymanym od Klienta lub podobnym dokumencie przekazanym Bankowi.*
Signature Verification *Weryfikacja podpisów*	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. *Korespondencja otrzymana przez Bank faksem, pocztą, pocztą elektroniczną lub komunikatorem, z wyłączeniem wniosków MIFT, przechodzi weryfikację podpisu na podstawie informacji zawartych w dokumencie upoważnienia otrzymanym od Klienta lub podobnym dokumencie przekazanym Bankowi.*
Secure PDF *Bezpieczny PDF*	Encrypted emails are delivered to a regular mailbox as PDF documents that are 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. *Zaszyfrowane wiadomości email dostarczane są do głównej skrzynki odbiorczej jako dokumenty PDF, które otwierane są poprzez wprowadzenie prywatnego hasła. Zaszyfrowana jest zarówno treść wiadomości, jak i wszelkie dołączone pliki. Prywatne hasło można skonfigurować po odebraniu pierwszej bezpiecznej wiadomości email.*
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 through an encrypted TLS tunnel created by the connection. *Mandatory Transport Layer Security (MTLS) tworzy bezpieczne, prywatne połączenie email pomiędzy Bankiem a Klientem. Wiadomości email przesyłane są przez Internet, specjalnie utworzonym na ten cel, szyfrowanym protokołem TLS tunelem.*

Phone Authentication Methods *Metody Uwierzytelniania Połączeń Telefonicznych*	
PIN *PIN*	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *Klienci kontaktujący się z Bankiem telefonicznie są proszeni o wprowadzenie PIN-u w celu uwierzytelnienia autoryzowanego dostępu.*
Verification Questions *Pytania weryfikujące*	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. *Klienci kontaktujący się z Bankiem telefonicznie są proszeni przez przedstawiciela Banku o podanie prawidłowych odpowiedzi na pytania weryfikujące w celu uwierzytelnienia autoryzowanego dostępu.*

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

Dostępność opisanych powyżej Metod Uwierzytelniania jest różna na poszczególnych rynkach lokalnych.

3. Customer Responsibilities
Zakres obowiązków Klienta

3.1 Identifying Authorized Users: Customer is responsible for identifying: (i) all individuals acting on the 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.

Identyfikacja Upoważnionych Użytkowników: Klient jest odpowiedzialny za identyfikację: (i) wszystkich osób działających na Rachunkach w imieniu Klienta na poziomie jednostki dla wszystkich Usług i kanałów dostępu, oraz (ii) każdej osoby działającej w imieniu Klienta, która jest prawidłowo upoważniona przez Klienta do działania na Rachunku Klienta.

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.

Klient jest odpowiedzialny za przyznanie i monitorowanie wszelkich limitów transakcji przypisanych Klientowi i/lub jego użytkownikom oraz za zapewnienie, żeby te limity (a) nie przekraczały limitów zgodnie z wymogami wewnętrznych polityk Klienta oraz innych dokumentów autoryzacyjnych i normatywnych, takich jak Uchwały Zarządu Klienta, Upoważnienia, Pełnomocnictwa lub równoważne dokumenty, oraz (b) były prawidłowo wykazane we wszystkich kanałach dostępu i uprawnieniach użytkownika.

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 BE website for further information.

W niektórych krajach, przed przyznaniem dostępu umożliwiającego wykonywanie pewnych funkcji, osoby fizyczne (z uwzględnieniem ich Narzędzi Uwierzytelniających) muszą być zidentyfikowane przez Bank zgodnie z właściwymi wymogami przepisów dotyczących przeciwdziałania praniu pieniędzy. W celu uzyskania dalszych informacji prosimy kontaktować się ze swoim Doradcą w Departamencie Obsługi Klienta – CitiService lub odwiedzić stronę CitiDirect BE.

3.4 Safeguarding of Authentication Methods
Ochrona Metod Uwierzytelniania

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.

Klient jest odpowiedzialny za ochronę Metod Uwierzytelniania i Narzędzi Uwierzytelniających z zachowaniem najwyższego standardu staranności, a także za zapewnienie, że dostęp do Narzędzi Uwierzytelniających i ich dystrybucja są ograniczone wyłącznie do osób upoważnionych przez Klienta.

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.

Komunikaty wysłane przez osobę trzecią: Jeżeli Klient stosuje Narzędzie Uwierzytelniające do celów identyfikacji i uwierzytelniania swoich Komunikatów jako pochodzących od niego jako podmiotu prawnego, Klient jest odpowiedzialny za zachowanie pełnej kontroli nad używaniem tych Narzędzi Uwierzytelniających w trakcie wysyłania Komunikatów do Banku, w tym również gdy te Komunikaty są wysyłane przez aplikacje i/lub systemy zarządzane przez osobę trzecią na rzecz Klienta. We wszystkich okolicznościach Bank (a) uzna każdy Komunikat otrzymany poprzez elektroniczny kanał dostępu, który został otrzymany przez Bank zgodnie z niniejszymi Procedurami Bezpieczeństwa i prawidłowo uwierzytelniony jako pochodzący od Klienta, za Komunikat przekazany przez Klienta oraz (b) może działać na podstawie każdego Komunikatu otrzymanego w imieniu Klienta zgodnie z niniejszymi Procedurami Bezpieczeństwa.

4. Data Integrity and Secured Communications
Integralność danych i bezpieczna komunikacja

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.

Klient będzie przesyłać dane do Banku oraz w inny sposób wymieniać Komunikaty z Bankiem, korzystając z Internetu, poczty, poczty elektronicznej i/lub faksu, które, co Klient rozumie, nie są (i) całkowicie bezpiecznymi środkami komunikacji i systemami doręczania oraz (ii) pod kontrolą Banku.

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.

Bank stosuje wiodące metody szyfrowania używane w branży (wskazane przez Bank), co pomaga zapewnić zachowanie poufności informacji i jej niezmienność podczas elektronicznej transmisji.

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.

Jeżeli Klient podejrzewa lub dowie się o awarii technicznej lub niewłaściwym lub potencjalnie oszukańczym dostępie do Usług lub kanałów dostępu lub Metod Uwierzytelniania Banku przez jakąkolwiek osobę (upoważnioną lub nieupoważnioną), Klient ma obowiązek niezwłocznie zawiadomić Bank o takim zdarzeniu. W razie niewłaściwego lub potencjalnie oszukańczego dostępu lub wykorzystania przez osobę upoważnioną, Klient powinien niezwłocznie podjąć działania w celu cofnięcia dostępu przyznanego tej upoważnionej osobie do Usług i kanałów dostępu Banku i uniemożliwienia jej korzystania z tych Usług i kanałów.

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.

Jeżeli Klient korzysta z programu do formatowania lub szyfrowania plików (udostępnionego przez Bank lub osobę trzecią) do obsługi formatowania i rozpoznawania danych i dyspozycji Klienta oraz działa na podstawie Komunikatów wymienianych z Bankiem, wówczas Klient będzie używał takiego oprogramowania wyłącznie w celu, w jakim zostało zainstalowane.

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.

Klient akceptuje, że Bank może zawiesić dostęp użytkownika do Usług wymagający użycia Narzędzi Uwierzytelniających lub odmówić takiego dostępu (i) w razie podejrzenia nieuprawnionego lub oszukańczego użycia Narzędzi Uwierzytelniających i/lub (ii) w celu ochrony Usług lub Narzędzi Uwierzytelniających.

5. Security Manager and Related Functions
Administrator Systemu i Powiązane Funkcje

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

Dla aplikacji dostępnych w CitiDirect BE (z wyjątkiem Certyfikatów Osobistych omówionych poniżej) Bank wymaga od Klienta ustanowienia funkcji „Administratora Systemu" odpowiedzialnego za:

5.1 Establishing and maintaining the access and entitlements of users (including Security Managers themselves) including activities such as to: (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);

Ustalanie i utrzymywanie dostępu i uprawnień użytkowników (w tym samych Administratorów Systemu), łącznie z działaniami takimi jak: (a) tworzenie, usuwanie lub modyfikowanie Profili użytkowników (w tym Profili Administratorów Systemu) i uprawnień (uwaga: nazwa użytkownika musi pasować do pomocniczego dokumentu identyfikacyjnego); (b) budowanie profili dostępu, które definiują funkcje i dane dostępne dla poszczególnych użytkowników; (c) włączanie i wyłączanie narzędzi uwierzytelniających stosowanych podczas logowania; oraz (d) przyznawanie limitów transakcji (uwaga: te limity nie są monitorowane ani walidowane przez Bank, a Klient powinien monitorować te limity, aby zapewnić, że są one zgodne z wewnętrznymi politykami i wymogami Klienta, w tym między innymi określonymi przez Zarząd Klienta lub równoważnymi);

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;

Tworzenie i modyfikowanie wpisów w bibliotekach systemu utrzymywanych przez Klienta (np. bibliotekach beneficjentów lub szablonów płatności) i upoważnianie do tego innych użytkowników;

5.3 Modifying payment authorization flows;

Modyfikowanie schematów autoryzacji płatności;

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

Przypisywanie narzędzi uwierzytelniających generujących hasła w sposób dynamiczny lub innych narzędzi umożliwiających dostęp do systemu użytkownikom Klienta; oraz

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

Zawiadamianie Banku w przypadku jakiegokolwiek podejrzenia, że zostało naruszone bezpieczeństwo.

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.

Uwaga: Role i zadania Administratora Systemu mogą się różnić lub mogą nie mieć zastosowania na pewnych rynkach ze względu na wymogi regulacyjne i/lub możliwości operacyjne. Na tych rynkach Bank może żądać dodatkowych dokumentów i innych informacji od Klienta w celu pełnienia funkcji Administratora Systemu na rzecz Klienta.

6. Use of CitiDirect BE by Security Managers
Korzystanie z CitiDirect BE przez Administratorów Systemu

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.

Bank wymaga wskazania co najmniej dwóch (2) różnych osób, które będą wprowadzać i autoryzować dyspozycje w systemie, dlatego konieczne jest ustanowienie co najmniej dwóch Administratorów Systemu. Dwaj dowolni Administratorzy Systemu, działając razem mogą wydawać przez kanały dostępu dyspozycje i/lub potwierdzenia związane z każdą realizowaną funkcją Administratora Systemu lub w związku z komunikacją. Każda taka komunikacja, autoryzowana przez dwóch Administratorów Systemu, zostanie zaakceptowana i wykonana przez Bank oraz uznana za przekazaną przez Klienta. Bank zaleca wyznaczenie co najmniej trzech Administratorów Systemu w celu zapewnienia odpowiedniego wsparcia w wyjątkowych sytuacjach. Klient wskazuje swoich Administratorów Systemu na właściwym wniosku Bankowość Transakcyjna - Formularz Aktywacji. Administrator Systemu może również działać jako Administrator Systemu podmiotu trzeciego (np. jednostki powiązanej z Klientem) i egzekwować wszelkie związane z tym prawa (łącznie z ustalaniem uprawnień użytkowników danego podmiotu do Rachunków), bez jakiegokolwiek dalszego upoważnienia, jeżeli dany podmiot trzeci wystawia formularz Upoważnienie do dostępu (UAA) (lub inny sposób akceptowany przez Bank) dający Klientowi dostęp do jego Rachunków. Ma to zastosowanie wyłącznie do Rachunków, których dotyczy dane upoważnienie.

7. Use of CitiDirect BE by Security Officers (For Personal Certificates only)
Korzystanie z CitiDirect BE przez Administratorów Systemu (tylko dla Certyfikatów Osobistych)

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 removal 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.

Bank wymaga, aby dwie (2) różne osoby zarządzały certyfikatami cyfrowymi przypisanymi do osób („Certyfikaty Osobiste"). Dlatego wymagane jest współdziałanie dwóch Administratorów Systemu w celu przyznania i cofnięcia Certyfikatu Osobistego użytkownika, na potrzeby uwierzytelniania i zatwierdzania Komunikatów w kanałach dostępu. Bank zaleca wyznaczenie co najmniej trzech Administratorów Systemu w celu zapewnienia odpowiedniego wsparcia w wyjątkowych sytuacjach. Każdy Komunikat zatwierdzony Certyfikatami Osobistymi zostanie zaakceptowany i wykonany przez Bank oraz uznany za przekazany przez Klienta.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions