Security Procedures
Proceduri de securitate

1. Introduction
Introducere

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).

Aceste „Proceduri de securitate", astfel cum sunt menționate în secțiunea Comunicări ale Condițiilor Cadru privind Contul și Serviciile („CCCS") (sau alți termeni și condiții aplicabile), sunt concepute pentru a autentifica conectarea Clientului la canalele de conectivitate ale Băncii și pentru a verifica proveniența Comunicărilor dintre Bancă și Client în legătură cu următoarele Servicii sau canale de conectivitate (a căror disponibilitate poate varia la nivelul piețelor locale).

- CitiDirect® (including WorldLink®)
  CitiDirect® (inclusiv WorldLink®)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  Transfer de fonduri inițiate manual („MIFT")
- Interactive Voice Response ("IVR")
  Răspuns vocal interactiv („IVR")
- Email/Fax/Mail/Messenger/Phone with the Bank
  E-mail/Fax/Corespondență prin poștă/Serviciu de mesagerie/Apel telefonic cu Banca
- Other local electronic connectivity channels
  Alte canale de conectivitate electronică locale

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:

Aceste Proceduri de securitate se vor citi împreună cu CCCS și pot fi actualizate și comunicate Clientului la anumite intervale de timp, prin mijloace electronice sau prin alte mijloace, inclusiv, dar fără a se limita la, postarea actualizărilor aduse Procedurilor de securitate pe CitiDirect. Cu excepția cazului în care este prevăzut altfel de lege, continuarea utilizării de către Client a oricăruia dintre Serviciile sau canalele de conectivitate amintite mai sus, după ce a fost înștiințat despre Procedurile de securitate actualizate va constitui acceptul Clientului cu privire la respectivele Proceduri de securitate actualizate. Aceste Proceduri de securitate abordează următoarele:

A. Authentication Methods
Metodele de autentificare

B. Customer Responsibilities
Responsabilitățile clientului

C. Data Integrity and Secured Communications
Integritatea datelor și Comunicările securizate

D. Security Manager and Related Functions
Managerul de securitate și funcțiile asociate

2. Authentication Methods
Metode de autentificare

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.

Procedurile de securitate includ anumite metode de autentificare sigure („Metode de autentificare"), care sunt utilizate pentru a identifica și verifica în mod unic autoritatea Clientului și/sau a oricăruia dintre utilizatorii săi autorizați de către Client în mod obișnuit prin intermediul unui mecanism sau a unei combinații de mecanisme, precum ID-ul de utilizator/perechi de parole, certificate digitale, date biometrice, token-uri de securitate (implementate prin intermediul unor echipamente hardware sau programe software), verificarea parafei/semnăturii și/sau dispozitive asociate Metodelor de autentificare (în mod colectiv, „Datele de autentificare"). Metodele de autentificare și Datele de autentificare asociate permit Băncii să verifice proveniența Comunicărilor primite de către Bancă.

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.

Mai multe informații cu privire la Metodele de autentificare pentru accesul la Servicii și/sau la canalele de conectivitate pot fi accesate pe site-ul web Ajutor pentru conectare CitiDirect. Clientul poate selecta în orice moment o Metodă de autentificare disponibilă. Pe parcursul implementării Serviciilor sau a canalelor de conectivitate, Banca poate configura o Metodă de autentificare implicită, pe care Clientul o poate schimba în orice moment cu o altă Metodă de autentificare disponibilă.

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

Pentru a accesa Serviciile și/sau canalele de conectivitate, sunt disponibile următoarele Metode de autentificare:

CitiDirect Authentication Methods *Metodele de autentificare CitiDirect*	
Biometrics *Datele biometrice*	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. *O metodă de autentificare digitală care utilizează trăsăturile fizice unice ale utilizatorului (cum ar fi o amprentă și recunoașterea facială), tehnologia biometrică fiind încorporată pe dispozitivul mobil al utilizatorului, și tehnici criptografice pentru a obține acces la CitiDirect. Datele referitoare la trăsăturile fizice nu sunt transferate către Bancă în momentul în care utilizatorul selectează această metodă de autentificare.*
Mobile Token (non-application based) *Token Mobil (fără aplicație)*	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. *O metodă digitală de autentificare mobilă, fără necesitatea utilizării unei aplicații dedicate (de ex. Token Mobil (fără aplicație)) care utilizează chei criptografice și autentificare biometrică (precum amprenta digitală sau recunoașterea facială) pentru a conecta dispozitivul mobil al utilizatorului la contul său CitiDirect prin intermediul browserului mobil al utilizatorului. Datele privind trăsăturile fizice nu sunt transferate către Bancă atunci când utilizatorul selectează această metodă de autentificare. Această metodă facilitează autentificarea cu mai mulți factori prin verificarea identității utilizatorului cu dispozitivul său mobil înregistrat.*
Challenge Response Token *Token pentru răspuns la interogare*	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. *Fie (i) un token sub forma unui program software bazat pe o aplicație mobilă (de ex., MobilePASS) fie (ii) un token fizic (de ex., SafeWord Card, Vasco), care se folosește în fiecare caz pentru a genera o parolă dinamică după autentificarea cu ajutorului unui cod PIN (de ex., codul PIN din 4 cifre). În momentul accesării CitiDirect, sistemul generează o interogare, iar token-ul utilizat și înregistrat în sistem generează o parolă de răspuns. Această metodă de autentificare, atunci când este combinată cu o parolă securizată, are ca rezultat autentificarea multi-factor.*
One-Time Password Token *Token cu parolă unică*	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. *Fie (i) un token sub forma unui program software bazat pe o aplicație mobilă (de ex., MobilePASS) fie (ii) un token fizic (de ex., SafeWord Card, Vasco), care se folosește pentru a genera o parolă dinamică după autentificarea cu ajutorului unui cod PIN (de ex. codul PIN din 4 cifre). Această parolă dinamică este introdusă în sistem pentru a obține acces.*

CitiDirect Authentication Methods ***Metodele de autentificare CitiDirect***	
Secure Password *Parola sigură*	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. *Un utilizator își introduce parola sigură pentru a accesa sistemul. O parolă sigură limitează de obicei capacitățile utilizatorului în sistem, de exemplu, permițând ca doar anumite informații să fie vizualizate de către utilizator. Această metodă de autentificare, atunci când este combinată cu un token pentru răspuns la interogare, are ca rezultat autentificarea multi-factor.*
SMS One-Time Code *Codul unic prin 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. *O parolă dinamică transmisă utilizatorilor prin SMS, după care utilizatorul introduce parola dinamică și o parolă sigură pentru a obține acces în sistem.*
Voice One-Time Code *Cod unic vocal*	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. *O parolă dinamică transmisă utilizatorilor prin intermediul unui apel vocal automat, după care utilizatorul introduce parola dinamică și o parolă sigură pentru a obține acces în sistem.*
Digital Certificates *Certificatele digitale*	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. 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. *Un certificat digital este o identificare electronică emisă de o autoritate de certificare autorizată pentru autentificare și autorizare. Certificatele digitale pot fi atribuite persoanelor juridice („Parafe corporative") sau persoanelor fizice („Certificate personale"). Clientul este responsabil pentru verificarea corespunzătoare a identității tuturor utilizatorilor de Certificate personale care acționează în numele Clientului în conformitate cu legislația locală.* *Banca și Clientul au obligația să utilizeze certificate digitale furnizate de persoane autorizate, pentru a se asigura că toate Comunicările schimbate prin intermediul unei conexiuni publice la internet sau o conexiune la internet nesigură sub altă formă sunt complet criptate și protejate.*

CitiConnect for Files Authentication Methods *Metodele de autentificare CitiConnect pentru fișiere*	
Digital Certificates *Certificatele digitale*	See description above. *Consultați descrierea de mai sus.*

CitiConnect for Files Authentication Methods *Metodele de autentificare CitiConnect pentru fișiere*	
IP Address Whitelist When Using CitiConnect *Lista albă cu adresele IP la utilizarea 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. *Anumite comunicări pe internet primite de către Bancă, de exemplu, prin intermediul unei rețele virtuale private (VPN), se pot baza, de asemenea, pe schimbul de informații realizat între părți folosind adrese de Protocol de Internet (IP) convenite în prealabil. Banca va accepta numai comunicările care provin de la adresa IP desemnată a Clientului și viceversa; iar Banca va transmite comunicări doar către adresa IP desemnată a Clientului și viceversa. Se folosește împreună cu metoda Certificat digital de mai sus.*

CitiConnect API Authentication Methods ***Metodele de autentificare Aplicația CitiConnect***	
Digital Certificates *Certificatele digitale*	See description above. *Consultați descrierea de mai sus.*
IP Address Whitelist When Using CitiConnect *Lista albă cu adresele IP la utilizarea CitiConnect*	See description above. *Consultați descrierea de mai sus.*

CitiConnect for SWIFT Authentication Methods ***Metodele de autentificare CitiConnect pentru SWIFT***	
Digital Certificates *Certificatele digitale*	See description above. Can be used in conjunction with SWIFT Authentication method below. *Consultați descrierea de mai sus. Se poate folosi împreună cu Metoda de autentificare SWIFT de mai jos.*

CitiConnect for SWIFT Authentication Methods *Metodele de autentificare CitiConnect pentru SWIFT*	
SWIFT Authentication *Autentificarea SWIFT*	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. 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. 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. *Comunicările trimise între Bancă și Client prin intermediul rețelei SWIFT, incluzând, dar fără a se limita la, informațiile referitoare la cont, ordinele de plată și instrucțiunile de modificare sau anulare a ordinelor respective, vor fi autentificate utilizând procedurile definite în Documentația contractuală SWIFT (cu modificările și completările ulterioare) care include, dar fără a se limita la, Termenii și condițiile generale și descrierea serviciului FIN sau astfel cum este prevăzut în alți termeni și condiții care pot fi stabilite de SWIFT. Banca nu este obligată să facă altceva în afară de ceea ce este inclus în procedurile SWIFT pentru a stabili expeditorul și autenticitatea acestor Comunicări.* *Banca nu este responsabilă pentru nicio eroare sau întârziere în sistemul SWIFT. Clientul este responsabil pentru transmiterea comunicărilor către Bancă în formatul și tipul prevăzute și specificate de SWIFT.* *Transmisiile și Comunicările trimise sau primite prin intermediul facilităților SWIFT se supun regulilor și reglementărilor SWIFT în vigoare, incluzând regulile privind calitatea de membru. Clientul este responsabil în ceea ce privește familiarizarea cu și respectarea standardelor privind mesageria SWIFT.*

SWIFT Authentication Method ***Metoda de autentificare SWIFT***	
SWIFT Authentication (Direct Connection for Financial Institutions) *Autentificarea SWIFT (conexiune directă pentru instituții financiare)*	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. 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. 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. *Comunicările trimise între Bancă și Client prin intermediul rețelei SWIFT, incluzând, dar fără a se limita la, informațiile referitoare la cont, ordinele de plată și instrucțiunile de modificare sau anulare a ordinelor respective, vor fi autentificate utilizând procedurile definite în Documentația contractuală SWIFT (cu modificările și completările ulterioare) care include, dar fără a se limita la, Termenii și condițiile generale și descrierea serviciului FIN sau astfel cum este prevăzut în alți termeni și condiții care pot fi stabilite de SWIFT. Banca nu este obligată să facă altceva în afară de ceea ce este inclus în procedurile SWIFT pentru a stabili expeditorul și autenticitatea acestor Comunicări.* *Banca nu este responsabilă pentru nicio eroare sau întârziere în sistemul SWIFT. Clientul este responsabil pentru transmiterea comunicărilor către Bancă în formatul și tipul prevăzute și specificate de SWIFT.* *Transmisiile și Comunicările trimise sau primite prin intermediul facilităților SWIFT se supun regulilor și reglementărilor SWIFT în vigoare, incluzând regulile privind calitatea de membru. Clientul este responsabil în ceea ce privește familiarizarea cu și respectarea standardelor privind mesageria SWIFT.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Semnătura digitală/electronică Metode de autentificare pentru depunerea documentelor electronice***	
Digital Signature *Semnătura digitală*	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. *Un tip de semnătură electronică care se folosește de certificate digitale pentru a valida autenticitatea și integritatea unei semnături, a unui mesaj, a unui program software sau a unui document digital.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Semnătura digitală/electronică Metode de autentificare pentru depunerea documentelor electronice***	
Electronic Signature *Semnătura electronică*	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. *Un simbol electronic atașat unui contract sau altei evidențe, unic și utilizat de o persoană cu intenția de a semna. Semnăturile electronice pot fi stabilite sub formă de cuvinte, litere, cifre, simboluri, un clic pe un buton de pe un site web, încărcarea unei reproduceri sau scanarea unei semnături fizice, semnarea pe un ecran tactil sau exprimarea acordului privind orice termeni și condiții prin mijloace electronice. Creată sub controlul exclusiv al persoanei care o folosește, aceasta este anexată sau asociată în mod logic cu un mesaj de date, în măsură să identifice persoana care își exprimă consimțământul cu privire la mesajul de date și să certifice consimțământul acesteia. O asemenea Semnătură electronică ar fi transmisă Băncii prin intermediul canalelor electronice ale Băncii și în conformitate cu Metodele de autentificare asociate, descrise mai sus.*

Manual Initiated Funds Transfer (MIFT) Authentication Method ***Metoda de autentificare Transfer de fonduri inițiate manual (MIFT)***	
MIFT Authentication *Autentificarea 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. 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. *Transferul de fonduri inițiat manual (MIFT), inclusiv modificările, rechemările sau anulările instrucțiunilor manuale precedente, se poate realiza prin fax sau scrisoare sau încărcare în CitiDirect. Nu toate aceste forme sunt acceptate în toate țările. Inițiatorii sunt persoanele desemnate de către Client, care sunt autorizate să inițieze tranzacții în conformitate cu restricțiile care, dacă există, sunt identificate de către Client. Confirmatorii sunt persoanele desemnate de către Client, pe care Banca le poate suna înapoi, la discreția sa, pentru confirmarea instrucțiunilor inițiate manual pentru transferurile de fonduri.* *În anumite țări, numerele de telefon mobil nu sunt acceptate ca numere pentru returnarea apelului. Mai multe detalii sunt prevăzute în Ghidul de utilizare specific țării , Formularul global privind autorizarea tranzacțiilor manuale sau Formularul de numire universală. MIFT este destinat utilizării de către Client ca metodă pentru situații neprevăzute în vederea comunicării instrucțiunilor către Bancă.*

Mail, Fax, Email and Messenger Authentication Methods ***Metodele de autentificare corespondență poștală, fax, e-mail și servicii de mesagerie***	
Seal Image Verification *Verificarea cu imagina parafei*	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. *Corespondența primită de către Bancă prin fax, corespondență poștală, e-mail sau servicii de mesagerie, cu excepția solicitărilor MIFT, este verificată și colaționată cu atenția cuvenită, pe baza imaginii parafei conținute în documentul de autorizare a Clientului sau în documente asemănătoare furnizate Băncii.*
Signature Verification *Verificarea semnăturii*	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. *Corespondența primită de către Bancă prin fax, corespondență poștală, e-mail sau servicii de mesagerie, cu excepția solicitărilor MIFT, este verificată prin semnătură în baza informațiilor conținute în documentul de autorizare a Clientului sau în documente asemănătoare furnizate Băncii.*
Secure PDF *PDF securizat*	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. *E-mail-urile criptate sunt transmise către o cutie poștală electronică obișnuită, sub formă de documente PDF, care sunt deschise introducând o parolă privată. Atât corpul mesajului, cât și orice fișier atașat sunt criptate. O parolă privată poate fi configurată la momentul recepționării primului e-mail securizat primit.*
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. *Securitatea obligatorie a nivelului de transport (MTLS) creează ceea ce ar fi o conexiune de e-mail privată, securizată, între Bancă și Client. E-mail-urile transmise utilizând acest canal sunt trimise prin Internet prin intermediul unui tunel TLS criptat, creat de conexiune.*

Phone Authentication Methods ***Metodele de autentificare telefonice***	
PIN *PIN*	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *Clienților care contactează Banca pe cale telefonică li se solicită să introducă un cod PIN pentru a valida accesul autorizat.*
Verification Questions *Întrebările de verificare*	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. *Clienților care contactează Banca pe cale telefonică li se solicită din partea reprezentanților serviciului Băncii să ofere răspunsuri verbale corecte la întrebările de verificare pentru a valida accesul autorizat.*

The availability of Authentication Methods described above varies based on local markets.
Disponibilitatea Metodelor de autentificare descrise mai sus variază în funcție de pieţele locale.

3. Customer Responsibilities
Responsabilitățile clientului

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.

Identificarea utilizatorilor autorizați: Clientul este responsabil pentru identificarea: (i) tuturor persoanelor fizice care operează pe Cont (Conturi) în numele Clientului - persoană juridică pentru toate Serviciile și canalele de conectivitate și (ii) fiecărei persoane care acționează în numele Clientului ca fiind autorizată corespunzător de către Client să opereze pe Contul Clientului.

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.

Clientul este responsabil de atribuirea și monitorizarea oricăror limite de tranzacție alocate Clientului și/sau utilizatorilor săi și de a se asigura că aceste limite (a) nu depășesc limitele prevăzute de politicile interne ale Clientului și de alte autorizații și documente constitutive, cum ar fi deciziile Consiliului de administrație al Clientului, Mandatele acordate Băncii, Procura sau un document echivalent și (b) se reflectă în mod corespunzător pe toate canalele de conectivitate și cu privire la drepturile utilizatorilor.

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.

Anumite jurisdicții pot cere ca persoanele fizice (și Datele de autentificare corespunzătoare ale acestora) să fie identificate de către Bancă în conformitate cu cerințele legislației privind combaterea spălării banilor aplicabile, înainte de a acorda acces pentru îndeplinirea anumitor funcții. Vă rugăm să contactați Reprezentantul Serviciului Clienți sau să vizitați site-ul web CitiDirect pentru informații suplimentare.

3.4 Safeguarding of Authentication Methods
Protejarea Metodelor de autentificare

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.

Clientul este responsabil pentru protejarea Metodelor de autentificare și a Datelor de autentificare cu cel mai înalt standard de grijă și diligență și pentru a se asigura că accesul și distribuirea Datelor de autentificare se limitează exclusiv la persoanele care au fost autorizate de către Client.

Comunicările trimise de către o terță parte: În cazul în care Clientul utilizează Date de autentificare pentru a identifica și autentifica anumite Comunicări care îi aparțin, provenind din partea sa în calitate de persoană juridică, Clientul este responsabil pentru exercitarea controlului deplin asupra utilizării acestor Date de autentificare, atunci când trimite Comunicări către Bancă, inclusiv în situația în care Comunicările sunt trimise de aplicațiile și/sau sistemele gestionate de către o terță parte în numele Clientului. În toate circumstanțele, Banca va (a) considera orice Comunicare pe care o primește prin intermediul unui canal de conectivitate electronică, care a fost primită de către Bancă în conformitate cu aceste Proceduri de securitate, autentificată în mod corespunzător drept provenind de la Client, ca fiind o Comunicare dispusă de către Client și (b) poate acționa în sensul oricărei Comunicări pe care o primește în numele Clientului în conformitate cu aceste Proceduri de securitate.

4. Data Integrity and Secured Communications *Integritatea datelor și Comunicările securizate*

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.

Clientul va transmite date către Bancă și va efectua schimburi de comunicări prin intermediul internetului, al serviciilor poștale, e-mailului și/sau faxului, înțelegând că aceste mijloace de comunicare și livrare (i) nu sunt în mod necesar sisteme sigure de transmitere a informațiilor și (ii) nu se află sub controlul Băncii. Clientul înțelege, de asemenea, că, în cazul în care utilizatorii săi au dreptul de a accesa servicii de Open Banking și/sau platforme similare operate de terți, în afara sistemelor Citi, datele Clientului pot fi transmise prin intermediul acestor platforme terțe, care nu se află sub controlul Băncii.

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.

Banca utilizează metode de criptare de vârf la nivelul industriei (astfel cum este stabilit de către Bancă), care ajută la asigurarea păstrării confidențialității informațiilor și la prevenirea modificării acestora pe parcursul tranzitului electronic.

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.

În cazul în care Clientul suspectează sau ia la cunoștință o defecțiune tehnică sau orice accesare sau utilizare necorespunzătoare sau potențial frauduloasă în ceea ce privește Serviciile sau canalele de conectivitate ale Băncii sau Metodele de autentificare, din partea oricărei persoane (indiferent dacă este vorba despre o persoană autorizată sau nu), Clientul va înștiința cu promptitudine Banca despre un asemenea eveniment. În eventualitatea accesării sau utilizării necorespunzătoare sau potențial frauduloase de către o persoană autorizată, Clientul trebuie să ia măsuri imediate pentru a înceta accesarea și utilizarea Serviciilor sau Canalelor de conectivitate ale Băncii.

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.

În cazul în care Clientul utilizează programe software de formatare sau criptare a fișierelor (fie că sunt puse la dispoziție de către Bancă sau de către o terță parte) pentru a susține formatarea și recunoașterea datelor și instrucțiunilor Clientului și acționează în sensul Comunicărilor cu Banca, Clientul va folosi astfel de programe software exclusiv în scopul pentru care au fost instalate.

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.

Clientul acceptă faptul că Banca poate suspenda sau refuza accesul utilizatorilor la Servicii care necesită utilizarea Datelor de autentificare (i) în caz de suspiciune privind utilizarea neautorizată sau frauduloasă a Datelor de autentificare și/sau (ii) pentru a proteja Serviciile sau Datele de autentificare.

5. Security Manager and Related Functions *Managerul de securitate și funcțiile asociate*

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:

Pentru aplicațiile care pot fi accesate în CitiDirect (cu excepția Certificatelor personale discutate mai jos), Banca solicită Clientului să stabilească o funcție de „Manager de securitate". Managerii de securitate sunt responsabili pentru:

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);

Stabilirea și menținerea accesului și a drepturilor utilizatorilor (inclusiv pentru Managerii de securitate înșiși), incluzând activități precum: (a) crearea, ștergerea sau modificarea Profilurilor utilizatorilor (inclusiv profilurile Managerilor de securitate) și drepturile acordate (Rețineți că numele de utilizator trebuie să fie în conformitate cu documentele justificative de identificare); (b) realizarea profilurilor de acces, care definesc funcțiile și datele disponibile pentru utilizatorii individuali; (c) activarea și dezactivarea datelor de autentificare pentru conectarea utilizatorilor; și (d) atribuirea limitelor de tranzacție (Rețineți că aceste limite nu sunt monitorizate sau validate de către Bancă, iar Clientul trebuie să monitorizeze aceste limite pentru a se asigura că acestea respectă politicile și cerințele interne ale Clientului, inclusiv, dar fără a se limita la, cele stabilite de către Consiliul de administrație al Clientului sau un organism echivalent);.

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;

Crearea și modificarea înregistrărilor în bibliotecile menținute de către Client (cum ar fi plățile cu format prestabilit și bibliotecile neficiarilor) și autorizarea altor utilizatori să facă același lucru;

5.3 Modifying payment authorization flows;

Modificarea fluxurilor de autorizare a plăților;

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

Alocarea datelor de autentificare cu parole dinamice sau a altor date de autentificare sau parole de acces la sistem pentru utilizatorii Clientului;

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

Sesizarea Băncii, dacă există vreun motiv de suspiciune că securitatea a fost compromisă; și

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

Gestionarea și procurarea certificatelor digitale și autorizarea altor utilizatori să facă același lucru.

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.

Vă rugăm să rețineți că: Rolurile și responsabilitățile Managerilor de securitate pot varia sau este posibil să nu fie aplicabile pe anumite piețe, ca urmare a cerințelor de reglementare și/sau a capacităților operaționale. Pe piețele respective, Banca poate solicita o documentație suplimentară și alte informații de la Client pentru îndeplinirea funcțiilor de Manager de securitate în numele Clientului.

6. Use of CitiDirect and CitiConnect by Security Managers *Utilizarea CitiDirect de către Managerii de securitate*

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.

Banca solicită desemnarea a două (2) persoane separate care să introducă și să autorizeze instrucțiuni; prin urmare, sunt necesari minim doi Manageri de securitate. Oricare doi Manageri de securitate, care acționează împreună, sunt în măsură să emită instrucțiuni și/sau confirmări prin intermediul canalelor de conectivitate în legătură cu orice funcție de Manager de securitate sau în legătură cu facilitarea comunicărilor. Orice astfel de comunicări, atunci când sunt autorizate de către doi Manageri de securitate, vor fi acceptate și onorate de către Bancă și considerate a fi transmise de către Client. Banca recomandă desemnarea a cel puțin trei Manageri de securitate pentru a asigura o acoperire adecvată. Clientul va desemna Managerii de securitate ai Clientului pe Formularul de înrolare pentru canalele de conectivitate TTS. Totodată, un Manager de securitate al Clientului poate să acționeze și în calitate de Manager de securitate pentru o entitate terță (de exemplu, o societate afiliată a Clientului) și să-și exercite toate drepturile care se referă la aceasta (inclusiv numirea de utilizatori pentru Contul (Conturile) respectivei entități terțe), fără nicio formalitate suplimentară, dacă respectiva entitate terță semnează un formular de Autorizare de acces universal (sau un alt formular de autorizare acceptabil Băncii), acordând Clientului acces la contul (conturile) sale. Acest lucru se aplică numai în legătură cu Contul (Conturile) care constituie obiectul autorizației relevante.

7. Use of CitiDirect by Security Officers (For Personal Certificates only) *Utilizarea CitiDirect de către responsabilii de securitate (numai pentru Certificatele personale)*

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.

Banca solicită desemnarea a două (2) persoane separate care să gestioneze certificatele digitale atribuite persoanelor fizice („Certificatele personale"). Prin urmare, doi Responsabili de securitate sunt necesari pentru atribuirea și retragerea Certificatelor personale către/de la utilizatori, în scopul autentificării și autorizării Comunicărilor pe canalele de conectivitate. Banca recomandă desemnarea a cel puțin trei Responsabili de securitate pentru a asigura o acoperire adecvată. Orice Comunicări autorizate cu Certificate personale vor fi acceptate și onorate de către Bancă și considerate a fi transmise de către Client.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions