Treasury and Trade Solutions

Security Procedures
Bezpečnostné postupy

1. Introduction
Úvod

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).

Tieto "Bezpečnostné postupy" ako sú označené v článku "Komunikácia" v Rámcových podmienkach vedenia Účtov a poskytovania Služieb (ďalej len "MAST") (alebo v iných príslušných obchodných podmienkach), sú vytvorené za účelom autentifikácie prihlasovania Klienta do komunikačných kanálov Banky a tiež za účelom overenia pôvodu Komunikácie medzi Bankou a Klientom v spojení s nasledovnými Službami alebo komunikačnými kanálmi (dostupnosť ktorých sa môže líšiť v závislosti na jednotlivých miestnych trhoch).

- CitiDirect® (including WorldLink®)
  CitiDirect® (vrátane WorldLink®)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  Society for Worldwide Interbank Financial Telecommunication (ďalej len "SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  Manuálne iniciované prevody peňažných prostriedkov (ďalej len "MIFT")
- Interactive Voice Response ("IVR")
  Interaktívna hlasová odozva/Interactive Voice Response ("IVR")
- Email/Fax/Mail/Messenger/Phone with the Bank
  Email/Fax/Pošta/Kuriér/Telefón s Bankou
- Other local electronic connectivity channels
  Iné miestne elektronické komunikačné kanály

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:

Tieto Bezpečnostné postupy budú vykladané spolu s MAST a môžu byť z času na čas aktualizované a oznámené Klientovi elektronickými prostriedkami alebo iným spôsobom, vrátane najmä zverejnením aktualizovaných Bezpečnostných postupov v CitiDirect. Ak príslušné právne predpisy nestanovujú inak, pokračujúce používanie ktorejkoľvek z vyššie uvedených Služieb alebo akéhokoľvek komunikačného kanálu zo strany Klienta po upozornení o aktualizácii Bezpečnostných postupov, bude znamenať prijatie týchto aktualizovaných Bezpečnostných postupov zo strany Klienta. Tieto Bezpečnostné postupy pokrývajú nasledovné oblasti:

A. Authentication Methods
Autentifikačné metódy

B. Customer Responsibilities
Zodpovednosť Klienta

C. Data Integrity and Secured Communications
Integrita údajov a Zabezpečená Komunikácia

D. Security Manager and Related Functions
Systémový Administrátor a Súvisiace Funkcie

2. Authentication Methods *Autentifikačné metódy*

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.

Bezpečnostné postupy zahŕňajú určité bezpečné autentifikačné metódy (ďalej len "Autentifikačné metódy"), ktoré sa používajú na jednoznačnú identifikáciu a overenie oprávnenia Klienta a/alebo ktoréhokoľvek z jeho používateľov, poverených Klientom a to zvyčajne pomocou jedného alebo kombinácie viacerých mechanizmov, ako sú dvojica používateľského ID / hesla, digitálne certifikáty, biometria, bezpečnostné tokeny (vytvorené prostredníctvom hardvéru alebo softvéru), overenie pečate/podpisu a/alebo zariadenia spojené s Autentifikačnými metódami (spoločne ďalej ako „Identifikačné údaje"). Autentifikačné metódy a súvisiace Identifikačné údaje umožňujú Banke overiť pôvod Komunikácie prijatej Bankou.

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.

Ďalšie informácie, týkajúce sa Autentifikačných metód pre prístup k Službám a/alebo komunikačným kanálom sú dostupné na webovej stránke CitiDirect Login Help website. Klient si môže kedykoľvek zvoliť ktorúkoľvek dostupnú Autentifikačnú metódu. Počas implementácie Služieb alebo komunikačných kanálov môže Banka nastaviť predvolenú Autentifikačnú metódu, ktorú môže Klient kedykoľvek zmeniť na inú dostupnú Autentifikačnú metódu.

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

Na prístup k službám a/alebo komunikačným kanálom sú k dispozícii nasledujúce Autentifikačné metódy:

CitiDirect Authentication Methods *CitiDirect Autentifikačné metódy*	
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. Physical trait data is not transferred to the Bank when the user selects this authentication method. *Metóda digitálneho overovania, ktorá využíva jedinečné fyzické vlastnosti používateľa (napríklad odtlačok prsta a rozpoznávanie tváre), zabudovanú biometrickú technológiu v mobilnom zariadení používateľa a kryptografické techniky na získanie prístupu k CitiDirect. Ak si používateľ zvolí túto metódu autentifikácie, údaje o fyzických vlastnostiach sa do Banky neprenášajú.*
Mobile Token (non-application based) *Mobilný token* *(nezaložený na aplikácii)*	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. *Digitálna, na aplikácii nezaložená metóda mobilnej autentifikácie (napr. Mobile Token – bez aplikácie), ktorá využíva kryptografické kľúče a biometrickú autentifikáciu (ako je odtlačok prsta a rozpoznávanie tváre) na prepojenie mobilného zariadenia používateľa s jeho účtom CitiDirect prostredníctvom mobilného prehliadača používateľa. Pri výbere tejto metódy autentifikácie sa údaje o fyzických znakoch neprenášajú do Banky. Táto metóda umožňuje viacfaktorovú autentifikáciu overením identity používateľa jeho registrovaným mobilným zariadením.*
Challenge Response Token *Token Výzva na odpoveď*	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. *Buď (i) softvérový token založený na mobilných aplikáciách (napríklad MobilePASS) alebo (ii) fyzický token (napr. SafeWord Card, Vasco), ktorý sa v každom prípade použije na vytvorenie dynamického hesla po autentifikácii pomocou PIN-u (napr. 4-miestneho pin-u). Pri prístupe k službe CitiDirect systém vygeneruje výzvu a prístupový kód je generovaný použitým tokenom, ktorý je následne zadaný do systému. Výsledkom tejto metódy overenia v kombinácii so zabezpečeným heslom je viacfaktorové overenie.*
One-Time Password Token *Token Jednorazové heslo*	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. *Buď (i) softvérový token založený na mobilných aplikáciách (napríklad MobilePASS) alebo (ii) fyzický token (napr. SafeWord Card, Vasco), ktorý sa v každom prípade použije na vytvorenie dynamického hesla po autentifikácii pomocou PIN-u (napr. 4-miestneho pin-u). Toto dynamické heslo je vložené do systému za účelom získania prístupu.*

CitiDirect Authentication Methods ***CitiDirect Autentifikačné metódy***	
Secure Password *Bezpečné Heslo*	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. *Užívateľ zadá svoje bezpečnostné heslo na prístup k systému. Bezpečnostné heslo zvyčajne obmedzuje možnosti používateľa v systéme, napríklad že je možné len zobrazovať určité informácie. Táto autentifikačná metóda spolu s overením prostredníctvom Token – Výzva na odpoveď predstavuje viacfaktorové overenie.*
SMS One-Time Code *SMS Jednorazový Kód*	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. *Dynamické heslo je doručené používateľovi prostredníctvom SMS, po ktorom používateľ zadá dynamické heslo a zabezpečené heslo na získanie prístupu do systému.*
Voice One-Time Code *Hlasový Jednorazový Kód*	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. *Dynamické heslo je doručené užívateľovi prostredníctvom automatizovaného telefonického hovoru, po ktorom užívateľ zadá dynamické heslo a zabezpečené heslo na získanie prístupu do systému.*
Digital Certificates *Digitálne Certifikáty*	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. *Digitálny certifikát je elektronickou identifikáciou a je vydaný schválenou certifikačnou autoritou, ktorý sa používa na overenie a autorizáciu. Digitálne certifikáty môžu byť priradené k právnickým osobám (ďalej len „Elektronická pečať") alebo fyzickým osobám (ďalej len „Osobný certifikát"). Klient je zodpovedný za riadne overenie totožnosti všetkých používateľov Osobných certifikátov, konajúcich v mene Klienta v súlade s miestnymi právnymi predpismi.* *Banka a Klient sú povinní používať digitálne certifikáty poskytované oprávnenými osobami, aby zabezpečili úplné šifrovanie a ochranu všetkej Komunikácie vymieňanej prostredníctvom verejného Internetového pripojenia alebo inak nezabezpečeného Internetového pripojenia.*

CitiConnect for Files Authentication Methods *CitiConnect for Files Autentifikačné metódy*	
Digital Certificates *Digitálne Certifikáty*	See description above. *Viď popis vyššie.*

CitiConnect for Files Authentication Methods *CitiConnect for Files Autentifikačné metódy*	
IP Address Whitelist When Using CitiConnect *Zoznam povolených IP Adries (whitelist) pri používaní 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. *Určitá Internetová komunikácia prijatá Bankou, napríklad prostredníctvom virtuálnej súkromnej siete (VPN), sa tiež môže spoliehať na to, že si strany vymieňajú informácie pomocou vopred dohodnutých adries internetového protokolu (IP). Banka bude akceptovať len Komunikáciu pochádzajúcu z určenej IP adresy Klienta a naopak; a Banka bude prenášať Komunikáciu len na určenú IP adresu Klienta a naopak. Môže byť použité v spojení so metódou Digitálnych Certifikátov uvedenou vyššie.*

CitiConnect API Authentication Methods ***CitiConnect API Autentifikačné metódy***	
Digital Certificates *Digitálne Certifikáty*	See description above. *Viď popis vyššie.*
IP Address Whitelist When Using CitiConnect *Zoznam povolených IP Adries (whitelist) pri používaní CitiConnect*	See description above. *Viď popis vyššie.*

CitiConnect for SWIFT Authentication Methods ***CitiConnect for SWIFT Autentifikačné metódy***	
Digital Certificates *Digitálne Certifikáty*	See description above. Can be used in conjunction with SWIFT Authentication method below. *Viď popis vyššie. Môže byť použité v spojení so SWIFT Autentifikačnou metódou uvedenou nižšie.*

CitiConnect for SWIFT Authentication Methods *CitiConnect for SWIFT Autentifikačné metódy*	
SWIFT Authentication *SWIFT Autentifikácia*	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. *Komunikácia, odoslaná medzi Bankou a Klientom prostredníctvom siete SWIFT, vrátane najmä údajov o účte, platobných príkazov a pokynov na zmenu alebo zrušenie takýchto príkazov bude overená s použitím postupov, definovaných v zmluvnej dokumentácii týkajúcej sa SWIFT-u (ktorá sa môže z času na čas meniť a dopĺňať) a ktorá zahŕňa najmä jej Všeobecné Obchodné Podmienky a Popis Služby FIN, alebo ktoré sú uvedené v ďalších obchodných podmienkach, ktoré môže SWIFT vydať. Banka nie je povinná urobiť nič iné ako to, čo je obsiahnuté v postupoch SWIFT na to, aby sa zistil odosielateľa autenticita takejto Komunikácie.* *Banka nezodpovedá za žiadne chyby alebo oneskorenia v systéme SWIFT. Klient zodpovedá za zasielanie komunikácie Banke vo formáte a type požadovanom a špecifikovanom zo strany SWIFT-u.* *Prenosy a Komunikácie odosielané alebo prijímané prostredníctvom zariadení SWIFT podliehajú platným pravidlám a predpisom SWIFT, vrátane pravidiel členstva. Klient je zodpovedný za oboznámenie sa s podmienkami pre zasielanie správ SWIFT a za ich dodržiavanie.*

SWIFT Authentication Method ***SWIFT Autentifikačné metódy***	
SWIFT Authentication (Direct Connection for Financial Institutions) *SWIFT Autentifikácia (Priamy prístup pre Finančné inštitúcie)*	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. *Komunikácia, odoslaná medzi Bankou a Klientom prostredníctvom siete SWIFT, vrátane najmä údajov o účte, platobných príkazov a pokynov na zmenu alebo zrušenie takýchto príkazov bude overená s použitím postupov, definovaných v zmluvnej dokumentácii týkajúcej sa SWIFT-u (ktorá sa môže z času na čas meniť a doplňať) a ktorá zahŕňa najmä jej Všeobecné Obchodné Podmienky a Popis Služby FIN, alebo ktoré sú uvedené v ďalších obchodných podmienkach, ktoré môže SWIFT vydať. Banka nie je povinná urobiť nič iné ako to, čo je obsiahnuté v postupoch SWIFT na to, aby sa zistil odosielateľa autenticita takejto Komunikácie.* *Banka nezodpovedá za žiadne chyby alebo oneskorenia v systéme SWIFT. Klient zodpovedá za zasielanie komunikácie Banke vo formáte a type požadovanom a špecifikovanom zo strany SWIFT-u.* *Prenosy a Komunikácie odosielané alebo prijímané prostredníctvom zariadení SWIFT podliehajú platným pravidlám a predpisom SWIFT vrátane pravidiel členstva. Klient je zodpovedný za oboznámenie sa s podmienkami pre zasielanie správ SWIFT a za ich dodržiavanie.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Digitálny/Electronický Podpis Autentifikačné metódy pre doručovanie elektronických dokumentov***	
Digital Signature *Digitálny Podpis*	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. *Druh elektronického podpisu, ktorý pomocou digitálnych certifikátov overuje pravosť a integritu podpisu, správy, softvéru alebo digitálneho dokumentu.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Digitálny/Elektronický Podpis Autentifikačné metódy pre doručovanie elektronických dokumentov***	
Electronic Signature *Electronický Podpis*	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. *Elektronický symbol pripojený k zmluve alebo inému záznamu, jedinečný a používaný osobou s úmyslom podpísať. Elektronické podpisy môžu byť zavedené vo forme slov, písmen, číslic, symbolov, kliknutia na tlačidlo na webovej stránke, načítania faxu alebo skenovania fyzického podpisu, podpisu na dotykovej obrazovke alebo súhlasu s akýmikoľvek obchodnými podmienkami elektronickými prostriedkami. Vytvorený pod výlučnou kontrolou osoby, ktorá ho používa, je logicky pripojený alebo spojený s dátovou správou a je spôsobilý identifikovať osobu, ktorá s dátovou správou súhlasí a potvrdzuje jej súhlas. Takýto Elektronický Podpis by sa Banke zasielal prostredníctvom elektronických kanálov Banky a v súlade s príslušnými Autentifikačnými metódami uvedenými vyššie.*

Manual Initiated Funds Transfer (MIFT) Authentication Method ***Manuálne iniciovaný prevod peňažných prostriedkov (MIFT) Autentifikačné metódy***	
MIFT Authentication *MIFT Autentifikácia*	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. *Manuálne iniciované prevody peňažných prostriedkov (MIFT), vrátane dodatkov, odvolaní alebo zrušení predchádzajúcich manuálnych pokynov je možné vykonať faxom alebo listom alebo nahrať do CitiDirect. Nie všetky formy sú podporované vo všetkých krajinách. Iniciátormi sú osoby určené Klientom, ktoré sú oprávnené iniciovať transakcie v súlade s obmedzeniami, ak sú stanovené a ktoré sú identifikované Klientom. Potvrdzovatelia sú osoby určené Klientom, ktorým môže Banka podľa vlastného uváženia zavolať späť za účelom potvrdenia manuálne iniciovaných prevodov finančných prostriedkov.* *V niektorých krajinách nie sú čísla mobilných telefónov akceptované ako čísla za účelom spätného volania. Ďalšie podrobnosti nájdete v príslušnej Používateľskej príručke Cash Management pre danú krajinu, vo formulári Global Manual Transaction Authorization alebo formulári Universal Nomination Form. MIFT má byť Klientom používaný ako metóda na zasielanie pokynov Banke v prípade výnimočných udalostí.*

Mail, Fax, Email and Messenger Authentication Methods *Pošta, Fax, Email a Messenger Autentifikačné metódy*	
Seal Image Verification *Overenie Odtlačku Pečate*	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. *Korešpondencia prijatá bankou prostredníctvom faxu, poštou, e-mailom alebo kuriérom, s výnimkou požiadaviek MIFT, sa overuje a porovnáva s náležitou starostlivosťou na základe odtlačku pečate, ktoré sa nachádza v poverovacom dokumente Klienta alebo podobnom dokumente poskytnutom Banke.*
Signature Verification *Overenie Podpisu*	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. *Korešpondencia prijatá bankou prostredníctvom faxu, poštou, e-mailu alebo kuriérom, s výnimkou žiadostí MIFT, je overovaná prostredníctvom overenia podpisu na základe informácií uvedených v poverovacom dokumente Klienta alebo v podobnom dokumente poskytnutom Banke.*
Secure PDF *Zabezpečené 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. *Šifrované e-maily sa doručujú do bežnej poštovej schránky ako dokument vo formáte PDF, ktorý sa otvorí zadaním súkromného hesla, pričom telo správy, ako aj všetky pripojené súbory sú šifrované. Po prijatí prvého zabezpečeného e-mailu sa môže nastaviť súkromné heslo.*
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) vytvára zabezpečené a súkromné e-mailové spojenie medzi Bankou a Klientom. E-mail odoslaný pomocou tohto kanála sa posiela Internetom cez šifrovaný TLS tunel vytvorený pripojením.*

Phone Authentication Methods *Telefón Autentifikačné metódy*	
PIN *PIN*	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *Klienti, ktorí kontaktujú Banku telefonicky, sú vyzvaní na zadanie kódu PIN na overenie autorizovaného prístupu.*
Verification Questions *Overovacie Otázky*	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. *Klienti, ktorí kontaktujú Banku telefonicky, sú vyzvaní zástupcami jednotlivých služieb Banky, aby poskytli správne slovné odpovede na overovacie otázky s cieľom overenia autorizovaného prístupu.*

The availability of Authentication Methods described above varies based on local markets.
Dostupnosť Autentifikačných metód uvedených vyššie môže byť rôzna na jednotlivých miestnych trhoch.

3. Customer Responsibilities
Zodpovednosť 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.

Identifikácia Oprávnených Používateľov: Klient je zodpovedný za identifikáciu: (i) všetkých osôb konajúcich s Účtami v mene Klienta na úrovni jeho subjektu pre všetky Služby a komunikačné kanály a (ii) každej osoby konajúcej v mene Klienta, ktorá bola riadne oprávnená Klientom nakladať s Účtom 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 je zodpovedný za stanovenie a sledovanie akýchkoľvek transakčných limitov pridelených Klientovi a/alebo jeho používateľom a za zabezpečenie toho, aby tieto limity (a) neprekročili limity požadované internými predpismi Klienta a inými splnomocňovacími a konštitutívnymi dokumentmi, ako sú rozhodnutia Predstavenstva Klienta, Bankové poverenia, Plnomocenstvá alebo ekvivalentný dokument a (b) sa náležite odrážajú vo všetkých komunikačných kanáloch a oprávneniach používateľov.

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.

Niektoré jurisdikcie môžu vyžadovať, aby boli jednotlivci (a ich zodpovedajúce údaje) identifikovaní Bankou v súlade s požiadavkami platných právnych predpisov v oblasti boja proti legalizácii príjmov z trestnej činnosti a to predtým, ako im bude poskytnutý prístup k používaniu určitých funkcií. Pre ďalšie informácie prosím kontaktujte zástupcu služieb klientom alebo navštívte webovú stránku CitiDirect website.

3.4 Safeguarding of Authentication Methods
Bezpečnosť Autentifikačných metód

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.

Klient je zodpovedný za zabezpečenie Autentifikačných metód a Identifikačných údajov s najvyššou úrovňou starostlivosti a za zabezpečenie toho, aby prístup k Identifikačným údajom a ich odosielanie bolo obmedzené iba na osoby, ktoré boli na to Klientom oprávnené.

Komunikácia zasielaná tretími stranami: Ak Klient používa Identifikačné údaje na identifikáciu a autentifikáciu svojej Komunikácie, ktoré pochádzajú od neho ako právnickej osoby, je zodpovedný za zabezpečenie úplnej kontroly nad používaním týchto Identifikačných údajov pri zasielaní Komunikácie do Banky a to aj v prípade, keď je táto Komunikácia zasielaná prostredníctvom aplikácií a/alebo systémov, ktoré sú spravované treťou stranou v mene Klienta. Za každých okolností bude Banka (a) považovať akúkoľvek Komunikáciu, ktorú obdrží prostredníctvom elektronických komunikačných kanálov, za takú, ktorá bola prijatá Bankou v súlade s týmito Bezpečnostnými postupmi, náležite overenú ako pochádzajúcu od Klienta, a ako Komunikáciu inštruovanú zo strany Klienta a (b) oprávnená konať na základe akejkoľvek Komunikácie, ktorú prijme v mene Klienta v súlade s týmito Bezpečnostnými postupmi.

4. Data Integrity and Secured Communications *Integrita údajov a Zabezpečená Komunikácia*

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.

Zákazník bude prenášať údaje a inak si vymieňať komunikáciu s Bankou prostredníctvom internetu, pošty, e-mailu a/alebo faxu, pričom Zákazník chápe, že tieto kanály (i) nie sú nevyhnutne bezpečné komunikačné a doručovacie systémy a (ii) nie sú pod kontrolou Banky. Zákazník ďalej chápe, že ak majú používatelia Zákazníka oprávnenie pristupovať k Open Banking a/alebo podobným platformám tretích strán mimo systémov Citi, údaje Zákazníka môžu byť prenášané cez takéto platformy tretích strán, ktoré nie sú pod kontrolou Banky.

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.

Banka využíva špičkové spôsoby šifrovania (stanovené Bankou), ktoré pomáhajú zabezpečiť, aby boli informácie zachované ako dôverné a aby počas elektronického prenosu neboli pozmenené.

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.

Ak má Klient podozrenie alebo sa dozvie o technickej poruche alebo akomkoľvek nesprávnom alebo potenciálne neoprávnenom prístupe k Službám Banky ku komunikačným kanálom alebo Autentifikačným metódam, alebo ich neoprávnenému použitiu akoukoľvek osobou (či už oprávnenou osobou alebo nie), tak takúto skutočnosť okamžite oznámi Banke. V prípade nesprávneho alebo potenciálne neoprávneného prístupu alebo použitia oprávnenou osobou by mal Klient okamžite podniknúť kroky na ukončenie prístupu takej oprávnenej osoby k službám Banky alebo komunikačným kanálom a k ich využívaniu.

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.

Ak Klient využíva formátovanie súborov, šifrovací softvér (či už poskytnutý Bankou alebo treťou stranou) na podporu formátovania a rozpoznávania údajov a pokynov Klienta a vykonáva Komunikáciu s Bankou, potom Klient bude používať tento softvér výlučne len na ten účel, pre ktorý bol inštalovaný.

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 súhlasí s tým, že Banka môže pozastaviť prístup užívateľov k Službám, ktoré vyžadujú používanie Identifikačných údajov (i) v prípade podozrenia z neoprávneného alebo podvodného používania Identifikačných údajov a/alebo (ii) v záujme ochrany Služieb alebo Identifikačných údajov.

5. Security Manager and Related Functions *Systémový Administrátor a Súvisiace Funkcie*

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:

Pri aplikáciách dostupných v CitiDirect a v CitiConnect (s výnimkou nižšie uvedených osobných certifikátov) Banka vyžaduje, aby Zákazník zriadil funkciu „Bezpečnostného manažéra". Bezpečnostní manažéri zodpovedajú za:

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);

Stanovenie a správa prístupov a oprávnení (vrátane samotných Systémových administrátorov) vrátane aktivít zahŕňajúcich: (a) vytváranie, odstraňovanie alebo zmena používateľských Profilov (vrátane Profilov Systémových Administrátorov) a prístupových oprávnení (zoberte prosím na vedomie, že meno používateľa musí byť v súlade s identifikačnými dokumentmi), (b) vytváranie prístupových profilov, ktoré definujú funkcie a údaje dostupné pre rôznych používateľov, (c) sprístupnenie a zrušenie prihlasovacích údajov používateľov, a (d) stanovovanie transakčných limitov (zoberte prosím na vedomie, že Banka tieto limity nesleduje ani neoveruje a Klient by mal tieto limity monitorovať, aby zabezpečil súlad s vnútornými predpismi a požiadavkami Klienta vrátane, najmä tých, ktoré sú prijaté predstavenstvom Klienta alebo iným príslušným orgánom);

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;

Vytváranie a úprava záznamov v knižniciach Klienta (ako sú predformátované platby a knižnice príjemcov platieb) a udeľovanie rovnakého oprávnenia ostatným používateľom;

5.3 Modifying payment authorization flows;

Úprava tokov oprávnení na vykonávanie platieb;

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

Prideľovanie údajov dynamického hesla alebo iných údajov alebo hesiel pre prístup k systému pre používateľov;

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

Oznamovanie Banke, ak existuje nejaký dôvod na podozrenie, že došlo k ohrozeniu bezpečnosti; a

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

Spravovanie a obstarávanie digitálnych certifikátov a oprávňovanie iných používateľov, aby tak robili.

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.

Na vedomie: Funkcie a zodpovednosti Systémových administrátorov sa môžu líšiť alebo nemusia byť uplatniteľné na určitých trhoch z dôvodu regulačných požiadaviek a/alebo prevádzkových schopností. Na takýchto trhoch môže Banka vyžadovať od Klienta dodatočnú dokumentáciu a ďalšie informácie na vykonávanie funkcií Systémových administrátorov v mene Klienta.

6. Use of CitiDirect and CitiConnect by Security Managers *Používanie CitiDirect a CitiConnect Bezpečnostnými manažérmi*

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.

Banka vyžaduje na zadávanie a autorizáciu inštrukcií dve (2) samostatné osoby; vzhľadom na to sa vyžadujú minimálne dvaja Systéméoví administrátori. Ktorýkoľvek dvaja Systéméoví administrátori, konajúci v zhode, sú oprávnení zadať pokyny a/alebo potvrdenia prostredníctvom komunikačných kanálov v súvislosti s akoukoľvek funkciou Systémového administrátora alebo v súvislosti s uľahčením komunikácie. Akákoľvek takáto Komunikácia, ak bude schválená dvoma Systémovými administrátormi, bude akceptovaná a vykonaná zo strany Banky a bude považovaná za Komunikáciu odoslanú Klientom. Banka odporúča ustanovenie najmenej troch Systémových administrátorov, aby bola zabezpečená prípadná záloha. Klient ustanoví svojich Systémových administrátorov na príslušnom formulári TTS na prístup ku komunikačným kanálom (TTS Channels Onboarding Form). Systémový administrátor Klienta môže byť zároveň aj Systémovým administrátorom pre subjekt tretej strany (napríklad dcérska spoločnosť Klienta) a vykonávať všetky s tým súvisiace práva (vrátane určenia používateľov Účtov tejto tretej strany) bez akéhokoľvek ďalšieho menovania, ak tento subjekt tretej strany vyplní formulár prístupu Universal Access Authority form (alebo inú formu splnomocnenia akceptovateľného pre Banku), ktorým udelí Klientovi prístup na tieto jeho účty. Toto platí to len v súvislosti s Účtami, na ktoré sa vzťahuje príslušné splnomocnenie.

7. Use of CitiDirect by Security Officers (For Personal Certificates only) *Používanie CitiDirect bezpečnostnými pracovníkmi (len pre osobné certifikáty)*

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.

Banka vyžaduje na správu digitálnych certifikátov priradených k fyzickým osobám (ďalej len "Osobné certifikáty") dve (2) samostatné osoby. Vzhľadom na to je potrebné, aby dvaja Systémový užívatelia na účely autentifikácie a autorizácie Komunikácie na komunikačných kanáloch prideľovali a odoberali používateľom Osobné certifikáty. Banka odporúča ustanovenie najmenej troch Systémových užívateľov, aby bola zabezpečená prípadná záloha. Akákoľvek Komunikácia, ak bude autorizovaná Osobnými certifikátmi, bude akceptovaná a vykonaná zo strany Banky a bude považovaná za Komunikáciu odoslanú Klientom.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions