Security Procedures
Prosedur Keamanan

1. Introduction
Pendahuluan

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).

Prosedur Keamanan ini, sebagaimana yang disebutkan dalam Ketentuan Induk untuk Rekening dan Layanan (MAST), atau syarat dan ketentuan rekening lainnya yang berlaku, dirancang untuk mengotentikasi nasabah yang login ke connectivity channels Bank dan untuk melakukan verifikasi terhadap asal komunikasi antara Bank dan Nasabah sehubungan dengan Layanan atau connectivity channels berikut (ketersediaan yang mungkin berbeda antar pasar):

- CitiDirect BE® (including WorldLink®)
  CitiDirect BE® (termasuk WorldLink®)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  Transfer Dana yang Dinisiasi Secara Manual("MIFT")
- Interactive Voice Response ("IVR")
  Tanggapan Suara Interaktif("IVR")
- Email/Fax/Mail/Messenger/Phone with the Bank
  Email/Fax/Mail/Messenger/Phone with the Bank
- Other local electronic connectivity channels
  Connectivity channels elektronik lokal lainnya

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:

Prosedur Keamanan ini harus dibaca bersama dengan MAST dan mungkin update dan saran kepada Nasabah dari waktu ke waktu melaui elektronik atau alat lainnya, termasuk tetapi tidak terbatas dengan memposting update pada Prosedur Keamanan dari CitiDirect BE. Kecuali kalau ditentukan lain secara hukum, Nasabah dapat terus menggunakan salah satu dari Layanan atau connectivity channel yang disebutkan setelah diinformasikan mengenai Prosedur Keamanan yang diperbaharui yang merupakan penerimaan Nasabah terhadap Prosedur Keamanan yang diperbaharui tersebut. Prosedur Keamanan ini mencakup yang berikut ini:

2. Authentication Methods
Metode Otentikasi

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.

Prosedur Keamanan ini mencakup metode otentikasi tertentu yang aman (Metode Otentikasi), yang digunakan untuk mengidentifikasi dan memverifikasi wewenang Nasabah dan/atau pengguna secara unik, biasanya melalui salah satu atau mekanisme seperti pasangan ID /kata sandi Pengguna, sertifikat digital, dan token keamanan biometrik. (Digunakan melalui perangkat keras atau perangkat lunak), verifikasi segel / tanda tangan, dan / atau perangkat yang terkait dengan Metode Otentikasi (secara kolektif disebut "Kredensial"). Metode Otentikasi dan Kredensial terkait memungkinkan Bank untuk memverifikasi asal Komunikasi yang diterima oleh 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.

Informasi lebih lanjut mengenai Metode Otentikasi untuk akses ke Layanan dan / atau connectivity channel dapat diakses di situs web Bantuan Login CitiDirect. Nasabah dapat kapan saja memilih Metode Otentikasi yang tersedia. Selama implementasi Layanan atau connectivity channel, Bank dapat mengatur Metode Otentikasi sebagai default, yang dapat diubah setiap saat oleh Nasabah ke Metode Otentikasi lain yang tersedia

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

Metode Otentikasi berikut sudah tersedia untuk mengakses layanan dan/atau connectivity channel:

CitiDirect BE Authentication Methods *CitiDirect BE Metode Otentikasi*	
Biometrics *Biometrik*	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. *Metode autentikasi digital yang memanfaatkan ciri-ciri fisik pengguna yang unik, (seperti sidik jari dan pengenalan wajah), teknologi biometrik bawaan pada perangkat seluler pengguna, dan teknik kriptografi untuk mendapatkan akses ke CitiDirect BE. Data sifat fisik tidak ditransfer ke Bank ketika pengguna memilih metode otentikasi ini.*
Challenge Response Token *Token Challenge Response*	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. *Baik (i) soft token berbasis aplikasi mobile (mis. MobilePASS) atau (ii) token fisik (mis. Kartu SafeWord, Vasco), yang dalam setiap kasus digunakan untuk menghasilkan kata sandi dinamis setelah diautentikasi dengan PIN (mis. 4 digit PIN). Saat mengakses CitiDirect BE, sistem menghasilkan tantangan dan kode sandi respons dihasilkan oleh token yang digunakan dan dimasukkan ke dalam sistem. Metode otentikasi ini, bila digabungkan dengan kata sandi yang aman menghasilkan autentikasi multifaktor.*
One-Time Password Token *Token Password Satu Kali*	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. *Baik (i) soft token berbasis aplikasi seluler (mis. MobilePASS); atau (ii) token fisik (mis. Kartu SafeWord, Vasco) yang digunakan untuk menghasilkan kata sandi dinamis setelah diautentikasi dengan PIN (mis. PIN 4 digit). Kata sandi dinamis ini dimasukkan ke dalam sistem untuk mendapatkan akses.*
Secure Password *Password yang Aman*	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. *Um usuário insere sua senha segura para acessar o sistema. Uma senha segura normalmente limita os recursos de um usuário no sistema, por exemplo, permitindo apenas que determinadas informações sejam visualizadas pelo usuário. Esse método de autenticação, quando combinado com um token de resposta ao desafio, resulta em autenticação multifator.*
SMS One-Time Code *Kode SMS Satu Kali*	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. *Kata sandi dinamis dikirim ke pengguna melalui SMS, setelah itu pengguna memasukkan kata sandi dinamis dan kata sandi aman untuk mendapatkan akses ke sistem.*
Voice One-Time Code *Kode Suara Satu Kali*	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. *Kata sandi dinamis yang dikirimkan kepada pengguna melalui panggilan suara otomatis, setelah itu pengguna memasukkan kata sandi dinamis dan kata sandi aman untuk mendapatkan akses ke sistem.*

Digital Certificates *Sertifikat Digital*	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. *Sertifikat digital adalah identifikasi elektronik yang dikeluarkan oleh otoritas sertifikat yang disetujui untuk otentikasi dan otorisasi. Sertifikat digital dapat dikaitkan dengan badan hukum perusahaan ("Segel Korporat") atau individu ("Sertifikat Pribadi"). Nasabah bertanggung jawab untuk memverifikasi dengan benar identitas semua pengguna Sertifikat Pribadi yang bertindak atas nama Nasabah sesuai dengan hukum setempat.* 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 dan Nasabah diharuskan untuk menggunakan sertifikat digital yang disediakan oleh orang yang berwenang, untuk memastikan semua Komunikasi yang dipertukarkan melalui koneksi Internet publik atau koneksi Internet yang tidak aman sepenuhnya dienkripsi dan dilindungi.*

CitiConnect for Files Authentication Methods ***CitiConnect for Files Metode Otentikasi***	
Digital Certificates *Sertifikat Digital*	See description above. *Lihat penjelasan di atas.*
IP Address Whitelist When Using CitiConnect *IP Address Whitelist ketika menggunakan 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. *Komunikasi Internet tertentu yang diterima oleh Bank, misalnya, melalui Virtual Private Network (VPN), juga dapat mengandalkan pihak yang bertukar informasi menggunakan alamat Protokol Internet (IP) yang telah disepakati sebelumnya. Bank hanya akan menerima komunikasi yang berasal dari alamat IP yang ditunjuk Nasabah, dan sebaliknya; dan Bank hanya akan mengirimkan Komunikasi ke alamat IP yang ditunjuk Nasabah, dan sebaliknya. Digunakan bersama dengan metode Sertifikat Digital di atas.*

CitiConnect API Authentication Methods ***CitiConnect API Metode Otentikasi***	
Digital Certificates *Sertifikat Digital*	See description above. *Lihat penjelasan di atas.*
IP Address Whitelist When Using CitiConnect *IP Address Whitelist ketika menggunakan CitiConnect*	See description above. *Lihat penjelasan di atas.*

CitiConnect for SWIFT Authentication Methods *CitiConnect SWIFT Metode Otentikasi*	
Digital Certificates *Sertifikat Digital*	See description above. Can be used in conjunction with SWIFT Authentication method below. *Lihat penjelasan di atas. Dapat digunakan untuk metode otentikasi SWIFT di bawah ini.*
SWIFT Authentication *Otentikasi 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. *Komunikasi yang dikirim antara Bank dan Nasabah melalui jaringan SWIFT, termasuk, tetapi tidak terbatas pada, informasi Rekening, pesanan pembayaran, dan instruksi untuk mengubah atau membatalkan pesanan tersebut, akan disahkan menggunakan prosedur yang ditentukan dalam Dokumentasi Kontrak SWIFT (sebagaimana diubah atau ditambah dari waktu ke waktu) yang mencakup tanpa batasan, Syarat dan Ketentuan Umum serta Uraian Layanan FIN atau sebagaimana tercantum dalam syarat dan ketentuan lain yang dapat ditetapkan oleh SWIFT. Bank tidak berkewajiban untuk melakukan apa pun selain dari apa yang terkandung dalam prosedur SWIFT untuk menetapkan pengirim dan keaslian Komunikasi ini.* 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 tidak bertanggung jawab atas kesalahan atau keterlambatan dalam sistem SWIFT. Nasabah bertanggung jawab untuk menyediakan komunikasi kepada Bank dalam format dan jenis yang diperlukan dan ditentukan oleh 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. *Transmisi dan Komunikasi yang dikirim atau diterima melalui fasilitas SWIFT tunduk pada aturan dan peraturan SWIFT yang berlaku, termasuk aturan keanggotaan. Nasabah bertanggung jawab untuk memahami dan mematuhi standar perpesanan SWIFT.*

SWIFT Authentication Method *SWIFT Metode Otentikasi*	
SWIFT Authentication (Direct Connection for Financial Institutions) *Otentikasi SWIFT (sambungan langsung untuk layanan keuangan)*	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. *Komunikasi yang dikirim antara Bank dan Nasabah melalui jaringan SWIFT, termasuk, tetapi tidak terbatas pada, informasi Rekening, pesanan pembayaran, dan instruksi untuk mengubah atau membatalkan pesanan tersebut, akan disahkan menggunakan prosedur yang ditentukan dalam Dokumentasi Kontrak SWIFT (sebagaimana diubah atau ditambah dari waktu ke waktu) yang mencakup tanpa batasan, Syarat dan Ketentuan Umum serta Uraian Layanan FIN atau sebagaimana tercantum dalam syarat dan ketentuan lain yang dapat ditetapkan oleh SWIFT. Bank tidak berkewajiban untuk melakukan apa pun selain dari apa yang terkandung dalam prosedur SWIFT untuk menetapkan pengirim dan keaslian Komunikasi ini.* 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 tidak bertanggung jawab atas kesalahan atau keterlambatan dalam sistem SWIFT. Nasabah bertanggung jawab untuk menyediakan komunikasi kepada Bank dalam format dan jenis yang diperlukan dan ditentukan oleh 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. *Transmisi dan Komunikasi yang dikirim atau diterima melalui fasilitas SWIFT tunduk pada aturan dan peraturan SWIFT yang berlaku, termasuk aturan keanggotaan. Nasabah bertanggung jawab untuk memahami dan mematuhi standar perpesanan SWIFT.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission *Metode Otentikasi Tanda Tangan /Digital/Elektronik untuk pengiriman dokumen elektronik*	
Digital Signature *Tanda Tangan Digital*	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. *Merupakan jenis tanda tangan elektronik yang menggunakan sertifikat digital untuk memvalidasi otentisitas dan integritas dari tanda tangan, pesan, perangkat lunak atau dokumen digital.*

Electronic Signature *Tanda Tangan Elektronik*	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. *Simbol elektronik yang dilampirkan pada kontrak atau catatan lain, unik dan digunakan oleh seseorang dengan maksud untuk menandatangani. Tanda tangan elektronik dapat dibuat dalam bentuk kata, huruf, angka, simbol, klik tombol di situs web, unggah faksimili atau pindaian tanda tangan fisik, masuk pada layar sentuh, atau menyetujui syarat dan ketentuan dengan cara elektronik. Dibuat di bawah kendali satu-satunya orang yang menggunakannya, itu secara logis dilampirkan atau dikaitkan dengan pesan data, mampu mengidentifikasi orang yang menyetujui pesan data dan mengesahkan persetujuan orang tersebut. Tanda Tangan Elektronik tersebut akan diserahkan kepada Bank melalui saluran elektronik Bank dan sesuai dengan Metode Otentikasi terkait yang dijelaskan di atas.*

Manual Initiated Funds Transfer (MIFT) Authentication Method ***Metode Otentikasi Transfer Dana yang Dinisiasi Secara Manual***	
MIFT Authentication *Otentikasi 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. *Transfer Dana yang Diprakarsai secara Manual (MIFT), termasuk amandemen, penarikan kembali, atau pembatalan instruksi manual sebelumnya, dapat dilakukan melalui faks atau surat atau mengunggah ke CitDuirct. Tidak semua formulir didukung di semua negara. Inisiator adalah orang yang ditunjuk oleh Nasabah yang berwenang untuk melakukan transaksi sesuai dengan batasan, jika ada, diidentifikasi oleh Nasabah. Konfirmer adalah orang yang ditunjuk oleh Nasabah sehingga Bank dapat menelepon kembali, atas kebijakannya sendiri, untuk konfirmasi instruksi yang diprakarsai secara manual untuk transfer dana.* 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. *Di negara tertentu, nomor telepon seluler tidak diterima sebagai nomor panggilan balik. Rincian lebih lanjut diberikan dalam Panduan Pengguna Manajemen Kas Negara yang berlaku, Otorisasi Transaksi Manual Global atau Formulir Nominasi Universal. MIFT akan digunakan oleh Nasabah sebagai metode kontingensi untuk mengkomunikasikan instruksi kepada Bank.*

Mail, Fax, Email and Messenger Authentication Methods *Metode Otentikasi dengan Surat, Fax, Email, dan Messenger*	
Seal Image Verification *Verifikasi Gambar Segel*	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. *Korespondensi diterima oleh Bank melalui faks, surat, email atau kurir, tidak termasuk permintaan MIFT, diverifikasi dan disusun dengan hati-hati berdasarkan gambar meterai yang terkandung dalam dokumen otoritas Nasabah atau dokumen serupa yang diberikan kepada Bank.*
Signature Verification *Verifikasi Tanda Tangan*	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. *Korespondensi yang diterima oleh Bank melalui faks, email, atau kurir, tidak termasuk permintaan MIFT, diverifikasi tanda tangan berdasarkan informasi yang terkandung dalam dokumen otoritas Nasabah atau dokumen serupa yang diberikan kepada Bank.*
Secure PDF *PDF yang Aman*	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. *Email terenkripsi dikirim ke kotak surat biasa sebagai dokumen PDF yang dibuka dengan memasukkan kata sandi pribadi. Badan pesan dan file lampiran apa pun dienkripsi. Kata sandi pribadi dapat diatur setelah menerima email aman pertama yang diterima.*
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) menciptakan apa yang akan menjadi koneksi email pribadi yang aman antara Bank dan Nasabah. Email yang dikirim menggunakan saluran ini dikirim melalui Internet melalui terowongan TLS terenkripsi yang dibuat oleh koneksi.*

Phone Authentication Methods *Metode Otentikasi Telepon*	
PIN *PIN*	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *Nasabah yang menghubungi Bank melalui telepon diminta untuk memasukkan PIN untuk memvalidasi akses resmi.*
Verification Questions *Verifikasi Pertanyaan*	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. *Nasabah yang menghubungi Bank melalui telepon diminta oleh perwakilan layanan Bank untuk memberikan tanggapan verbal yang benar terhadap pertanyaan verifikasi untuk memvalidasi akses resmi.*

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

Ketersediaan Metode Otentikasi seperti yang dijelaskan di atas berbeda beda tergantuang pasarnya.

3. Customer Responsibilities
Tanggung Jawab Nasabah

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.

Mengidentifikasi Pengguna yang sah: Nasabah bertanggung jawab untuk mengidentifikasi: (i) semua individu yang bertindak atas Rekening(-rekening) atas nama Nasabah pada tingkat entitas untuk semua Layanan dan Connectivity Channels, dan (ii) setiap orang yang bertindak atas nama Nasabah yang diberi kuasa oleh Nasabah untuk bertindak atas Rekening Nasabah.

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.

Nasabah bertanggung jawab untuk menetapkan dan memantau batas-batas transaksi apa pun yang diberikan kepada Nasabah dan / atau penggunanya dan memastikan bahwa batas-batas ini (a) tidak melebihi batas sebagaimana disyaratkan oleh kebijakan internal Nasabah dan otoritas lain dan dokumen konstitutif seperti Keputusan Direksi Nasabah, Mandat Bank, Surat Kuasa, atau dokumen yang setara, dan (b) tercermin secara memadai di semua Connectivity Channels dan hak pengguna.

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.

Yurisdiksi tertentu mungkin mengharuskan individu (dan Kredensial terkait) untuk diidentifikasi oleh Bank sesuai dengan persyaratan perundang-undangan AML yang berlaku sebelum memberikan akses untuk melakukan fungsi-fungsi tertentu. Silakan hubungi Perwakilan Layanan Nasabah Anda atau kunjungi situs web CitiDirect BE untuk informasi lebih lanjut.

3.4 Safeguarding of Authentication Methods

Perlindungan Metode Otentikasi

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.

Nasabah bertanggung jawab untuk melindungi Metode Otentikasi dan Kredensial dengan standar perawatan dan ketekunan tertinggi, dan memastikan bahwa akses ke dan distribusi Kredensial hanya terbatas pada orang-orang yang telah diberi wewenang oleh Nasabah.

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.

Komunikasi yang dikirim oleh pihak ketiga: Ketika Nasabah menggunakan Kredensial untuk

mengidentifikasi dan mengotentikasi Komunikasi mereka yang berasal dari mereka sebagai badan hukum, Nasabah bertanggung jawab untuk melakukan kontrol penuh atas penggunaan Kredensial tersebut saat mengirim Komunikasi ke Bank, termasuk di mana Komunikasi tersebut dikirim oleh aplikasi dan / atau sistem yang dikelola oleh pihak ketiga atas nama Nasabah. Dalam semua keadaan, Bank akan (a) menganggap Komunikasi apa pun yang diterimanya melalui Connectivity Channels elektronik, yang telah diterima oleh Bank sesuai dengan Prosedur Keamanan yang diautentikasi sebagaimana berasal dari Nasabah, sebagai Komunikasi yang diinstruksikan oleh Nasabah dan (b) dapat bertindak atas Komunikasi apa pun yang diterimanya atas nama Nasabah sesuai dengan Prosedur Keamanan yang diautentikasi sebagaimana berasal dari Nasabah, sebagaimana Komunikasi yang diinstruksikan oleh Nasabah dan (b) dapat bertindak berdasarkan Komunikasi apa pun yang diterimanya atas nama Nasabah sesuai dengan Prosedur Keamanan ini.

4. Data Integrity and Secured Communications
Integritas Data dan Komunikasi yang Aman

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.

Nasabah akan mentransmisikan data ke dan bertukar Komunikasi dengan Bank, menggunakan internet, surat, email dan / atau faks yang dipahami oleh Nasabah bukan (i) tentu saja mengamankan sistem komunikasi dan pengiriman, dan (ii) di bawah kontrol bank.

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, menggunakan metode enkripsi terkemuka di industri (sebagaimana ditentukan oleh Bank), yang membantu memastikan bahwa informasi dirahasiakan dan tidak berubah selama transit elektronik.

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.

Jika Nasabah mencurigai atau menjadi sadar akan kegagalan teknis atau akses yang tidak patut atau berpotensi curang ke atau penggunaan Layanan Bank atau Connectivity Channels atau Metode Otentikasi oleh siapa pun (baik orang yang berwenang atau tidak), Nasabah harus segera memberi tahu Bank kejadian seperti itu. Dalam hal akses atau penggunaan yang tidak patut atau kemungkinan penipuan oleh orang yang berwenang, Nasabah harus mengambil tindakan segera untuk menghentikan akses orang yang berwenang tersebut ke dan penggunaan Layanan Bank atau Connectivity Channels.

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.

Jika Nasabah menggunakan pemformatan file atau perangkat lunak enkripsi (baik yang disediakan oleh Bank atau pihak ketiga) untuk mendukung pemformatan dan pengakuan data dan instruksi Nasabah dan bertindak berdasarkan Komunikasi dengan Bank, Nasabah akan menggunakan perangkat lunak tersebut hanya untuk tujuan yang telah diinstal.

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.

Nasabah menerima bahwa Bank dapat menangguhkan atau menolak akses pengguna ke Layanan yang membutuhkan penggunaan Kredensial (i) jika ada dugaan penggunaan Kredensial yang tidak sah atau curang dan / atau (ii) untuk melindungi Layanan atau Kredensial tersebut.

5. Security Manager and Related Functions
Security Manager dan Fungsi Terkait

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:

Untuk aplikasi yang dapat diakses di CitiDirect BE (dengan pengecualian Sertifikat Pribadi yang dibahas di bawah), Bank mewajibkan Nasabah untuk membuat fungsi "Manajer Keamanan". Manajer Keamanan bertanggung jawab untuk:

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);

Menetapkan dan memelihara akses dan hak pengguna (termasuk Manajer Keamanan itu sendiri) termasuk kegiatan seperti: (a) membuat, menghapus, atau memodifikasi Profil pengguna (termasuk Profil Manajer Keamanan) dan hak kepemilikan (Perhatikan bahwa nama pengguna harus sejajar dengan dokumen identifikasi pendukung); (B) membangun profil akses yang mendefinisikan fungsi dan data yang tersedia untuk pengguna individu; (c) mengaktifkan dan menonaktifkan kredensial log-on pengguna; dan (d) menetapkan batas-batas transaksi (Perhatikan bahwa batas-batas ini tidak dipantau atau divalidasi oleh Bank dan Nasabah harus memantau batas-batas ini untuk memastikan mereka mematuhi kebijakan dan persyaratan internal Nasabah, termasuk tetapi tidak terbatas pada, yang ditetapkan oleh Nasabah Dewan Direksi atau yang setara);

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;

Membuat dan memodifikasi entri di perpustakaan yang dikelola Nasabah (seperti pembayaran yang telah diformat sebelumnya dan perpustakaan penerima manfaat) dan mengotorisasi pengguna lain untuk melakukan hal yang sama;

5.3 Modifying payment authorization flows;

Memodifikasi aliran otorisasi pembayaran;

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

Mengalokasikan kredensial kata sandi dinamis atau kredensial atau kata sandi akses sistem lainnya kepada pengguna Nasabah; dan

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

Memberitahu Bank, jika ada alasan untuk mencurigai bahwa keamanan telah dikompromikan.

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.

Harap dicatat: Peran dan tanggung jawab Manajer Keamanan dapat bervariasi atau tidak berlaku di pasar tertentu karena persyaratan peraturan dan / atau kemampuan operasional. Di pasar tersebut, Bank dapat meminta dokumentasi tambahan dan informasi lain dari Nasabah untuk melakukan fungsi Manajer Keamanan atas nama Nasabah.

6. Use of CitiDirect BE by Security Managers
Penggunaan CitiDirect BE oleh Security Managers

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 membutuhkan dua (2) individu yang terpisah untuk memasukkan dan mengesahkan instruksi; oleh karena itu, minimum dua Manajer Keamanan diperlukan. Dua Manajer Keamanan, yang bertindak bersama-sama, dapat memberikan instruksi dan / atau konfirmasi melalui Connectivity Channels sehubungan dengan fungsi Manajer Keamanan atau sehubungan dengan memfasilitasi komunikasi. Setiap komunikasi tersebut, ketika diizinkan oleh dua Manajer Keamanan, akan diterima dan ditindaklanjuti oleh Bank dan dianggap diberikan oleh Nasabah. Bank merekomendasikan penunjukan setidaknya tiga Manajer Keamanan untuk memastikan cadangan yang memadai. Nasabah harus menunjuk Manajer Keamanan Nasabah pada Formulir Onboarding TTS Channels. Manajer Keamanan Nasabah juga dapat bertindak sebagai Manajer Keamanan untuk entitas pihak ketiga (misalnya, afiliasi Nasabah) dan menggunakan semua hak yang terkait dengannya (termasuk penunjukan pengguna untuk Rekening entitas pihak ketiga itu) , tanpa penunjukan lebih lanjut, jika entitas pihak ketiga tersebut mengeksekusi formulir Otoritas Akses Universal (atau bentuk otorisasi lain yang dapat diterima oleh Bank) yang memberikan kepada Nasabah akses ke rekeningnya. Ini hanya berlaku sehubungan dengan Rekening yang dicakup dalam otorisasi yang relevan.

7. Use of CitiDirect BE by Security Officers (For Personal Certificates only)
Penggunaan CitiDirect BE oleh Security Officers (Hanya untuk Sertifikat Pribadi)

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 mewajibkan dua (2) individu terpisah untuk mengelola sertifikat digital yang dikaitkan dengan individu ("Sertifikat Pribadi"). Oleh karena itu, dua Petugas Keamanan diharuskan untuk menetapkan dan menghapus Sertifikat Pribadi kepada pengguna, dengan tujuan untuk mengotentikasi dan mengesahkan Komunikasi pada Connectivity Channels. Bank merekomendasikan penunjukan setidaknya tiga Petugas Keamanan untuk memastikan cadangan yang memadai. Setiap Komunikasi yang disahkan oleh Sertifikat Pribadi akan diterima dan ditindaklanjuti oleh Bank dan dianggap diberikan oleh Nasabah.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions