Security Procedures
Procedimentos de Segurança

1. Introduction
Introdução

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).

Esses "Procedimentos de Segurança", conforme referenciados na seção Comunicações dos Termos de Serviço e Conta Principal ("MAST") (ou outros termos e condições de contas aplicáveis), foram estabelecidos para autenticar o acesso do Cliente aos canais de conectividade do Banco e para verificar a origem das Comunicações entre o Banco e o Cliente relacionado com os Serviços ou canais de conectividade a seguir (cuja disponibilidade pode variar nos mercados locais).

- CitiDirect BE® (including WorldLink®)
  CitiDirect BE® (incluindo o WorldLink®)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  Sociedade de Telecomunicações Financeiras Interbancárias Mundiais ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  Transferência de fundos iniciada manualmente ("MIFT")
- Interactive Voice Response ("IVR")
  Resposta de Voz Interativa ("IVR")
- Email/Fax/Mail/Messenger/Phone with the Bank
  E-mail / fax / correio / mensageiro / telefone com o banco
- Other local electronic connectivity channels
  Outros canais locais de conectividade eletrônica

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:

Esses Procedimentos de Segurança devem ser lidos juntamente com o MAST e podem ser atualizados e informados periodicamente ao Cliente por meios eletrônicos ou outros, incluindo, entre outros, o envio de atualizações aos Procedimentos de Segurança no CitiDirect BE. Salvo disposição legal em contrário, o uso continuado do Cliente de qualquer um dos Serviços ou canais de conectividade acima mencionados após ser avisado dos Procedimentos de Segurança atualizados constituirá a aceitação do Cliente de tais Procedimentos de Segurança atualizados. Estes Procedimentos de Segurança cobrem o seguinte:

A. Authentication Methods
Métodos de autenticação

B. Customer Responsibilities
Responsabilidades do cliente

C. Data Integrity and Secured Communications
Integridade dos dados e comunicações segura

D. Security Manager and Related Functions
Usuário Master e funções relacionadas

2. Authentication Methods
Métodos de autenticação

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.

Os Procedimentos de Segurança incluem determinados métodos de autenticação segura ("Métodos de Autenticação") que são usados para identificar e verificar exclusivamente a autoridade do Cliente e / ou qualquer um dos seus usuários autorizados, normalmente por meio de um ou uma combinação de mecanismos, como ID do usuário / pares de senhas, certificados digitais, biometria, tokens de segurança (implantados via hardware ou software), verificação de selo / assinatura e / ou dispositivos associados aos Métodos de Autenticação (coletivamente, as "Credenciais"). Os Métodos de Autenticação e Credenciais associadas permitem ao Banco verificar a origem das Comunicações que recebe.

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.

Mais informações sobre os Métodos de Autenticação para acessar Serviços e / ou canais de conectividade podem ser acessadas em Ajuda de login do CitiDirect BE website. O Cliente pode selecionar um Método de Autenticação disponível a qualquer momento. Durante a implementação dos Serviços ou canais de conectividade, o Banco pode configurar um Método de Autenticação padrão, que o Cliente pode alterar a qualquer momento para outro método disponível:

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

Os seguintes Métodos de Autenticação estão disponíveis para acessar os serviços e / ou canais de conectividade:

CitiDirect BE Authentication Methods ***CitiDirect BE Métodos de autenticação***	
Biometrics *Biometria*	A digital authentication method that utilizes a user's unique physical traits, (such as a fingerprint and facial recognition), built-in biometric technology on the user's mobile device, and cryptographic techniques to gain access to CitiDirect BE. Physical trait data is not transferred to the Bank when the user selects this authentication method. *Um método de autenticação digital que usa as características físicas exclusivas de um usuário (como impressões digitais e reconhecimento facial), criado com tecnologia biométrica no dispositivo móvel do usuário e técnicas criptográficas para obter acesso ao CitiDirect BE. Os dados das características físicas não são transferidos para o banco quando o usuário seleciona esse método de autenticação.*

Challenge Response Token *Token de resposta ao desafio*	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. *(i) Um token de software baseado em aplicativo móvel (por exemplo, MobilePASS) ou (ii) um token físico (por exemplo, cartão SafeWord) que, em cada caso, é usado para gerar uma senha dinâmica após a autenticação com um PIN (por ex., de 4 dígitos). Ao acessar o CitiDirect BE, o sistema gera um desafio, e uma senha de resposta é gerada pelo token utilizado e digitada no sistema. Esse método de autenticação, quando combinado com uma senha segura, resulta em autenticação multifator.*
One-Time Password Token *Token de senha de uso único*	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. *(i) Um token de software baseado em aplicativo móvel (por exemplo, MobilePASS) ou (ii) um token físico (por exemplo, cartão SafeWord) que é usado para gerar uma senha dinâmica após a autenticação com um PIN (por ex., de 4 dígitos). Esta senha dinâmica é inserida no sistema para obter acesso.*
Secure Password *Senha segura*	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 *Código de uso único via 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. *Uma senha dinâmica é entregue a um usuário via SMS, em seguida o usuário digita a senha dinâmica e uma senha segura para obter acesso ao sistema.*
Voice One-Time Code *Código de uso único via voz*	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. *Uma senha dinâmica é fornecida a usuários via uma chamada de voz automatizada, em seguida o usuário digita a senha dinâmica e uma senha segura para obter acesso ao sistema.*

Digital Certificates *Certificados digitais*	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. *Um certificado digital é uma identificação eletrônica emitida por uma autoridade certificadora aprovada para autenticação e autorização. Os certificados digitais podem ser atribuídos a empresas corporativas ("Selos Corporativos") ou a indivíduos ("Certificados Pessoais"). O Cliente é responsável por verificar devidamente a identidade de todos os usuários de Certificados Pessoais agindo em nome do Cliente, de acordo com a lei local.* 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. *O Banco e o Cliente são obrigados a usar certificados digitais fornecidos por pessoas autorizadas, para garantir que todas as Comunicações trocadas via conexão pública à Internet ou por uma conexão não segura à Internet sejam totalmente criptografadas e protegidas.*

CitiConnect for Files Authentication Methods ***CitiConnect para Arquivos Métodos de autenticação***	
Digital Certificates *Certificados digitais*	See description above. *Veja a descrição acima.*
IP Address Whitelist When Using CitiConnect *Endereços de IP ista segura ao usar o 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. *Determinadas comunicações da Internet recebidas pelo Banco, por exemplo, por meio de uma Rede Virtual Privada (VPN), também podem confiar nas partes que trocam informações usando endereços de Protocolo da Internet (IP) pré-acordados. O Banco aceitará apenas as comunicações provenientes do endereço IP designado do Cliente e, da mesma forma, o Banco somente transmitirá Comunicações ao endereço IP designado do Cliente. Usado juntamente com o método de Certificado digital acima.*

CitiConnect API Authentication Methods ***CitiConnect API Métodos de autenticação***	
Digital Certificates *Certificados digitais*	See description above. *Veja a descrição acima.*

IP Address Whitelist When Using CitiConnect *Endereços de IP Lista segura ao usar o CitiConnect*	See description above. *VVeja a descrição acima.*

CitiConnect for SWIFT Authentication Methods *CitiConnect para SWIFT Métodos de autenticação*	
Digital Certificates *Certificados digitais*	See description above. Can be used in conjunction with SWIFT Authentication method below. *Veja a descrição acima. Pode ser usado juntamente com o método de autenticação SWIFT abaixo.*
SWIFT Authentication *Autenticação 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. *As comunicações enviadas entre o Banco e o Cliente pela rede SWIFT, incluindo, entre elas, informações da conta, pedidos de pagamento e instruções para alterar ou cancelar tais pedidos, serão autenticadas usando os procedimentos definidos na Documentação Contratual do SWIFT (conforme emendada ou complementada de tempos em tempos), que inclui, entre eles, os Termos e Condições Gerais e a Descrição do Serviço FIN, ou conforme estabelecido em outros termos e condições que possam ser estabelecidos pela SWIFT. O Banco não é obrigado a fazer nada além do que está contido nos procedimentos SWIFT para estabelecer o emissor e a autenticidade dessas Comunicações.* 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. *O Banco não é responsável por erros ou atrasos no sistema SWIFT. O Cliente é responsável por fornecer comunicações ao Banco no formato e tipo exigidos e especificados pela 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. *As transmissões e Comunicações enviadas ou recebidas por meio das instalações da SWIFT estão sujeitas às normas e regulamentos da SWIFT em vigor, incluindo as normas de associação. O Cliente se responsabiliza por se familiarizar e estar em conformidade com os padrões das mensagens SWIFT.*

SWIFT Authentication Method *SWIFT Métodos de autenticação*	
SWIFT Authentication (Direct Connection for Financial Institutions) *Autenticação SWIFT (conexão direta para instituições financeiras)*	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. *As comunicações enviadas entre o Banco e o Cliente pela rede SWIFT, incluindo, entre elas, informações da conta, pedidos de pagamento e instruções para alterar ou cancelar tais pedidos, serão autenticadas usando os procedimentos definidos na Documentação Contratual do SWIFT (conforme emendada ou complementada de tempos em tempos), que inclui, entre eles, os Termos e Condições Gerais e a Descrição do Serviço FIN, ou conforme estabelecido em outros termos e condições que possam ser estabelecidos pela SWIFT. O Banco não é obrigado a fazer nada além do que está contido nos procedimentos SWIFT para estabelecer o emissor e a autenticidade dessas Comunicações.* 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. *O Banco não é responsável por erros ou atrasos no sistema SWIFT. O Cliente é responsável por fornecer comunicações ao Banco no formato e tipo exigidos e especificados pela 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. *As transmissões e Comunicações enviadas ou recebidas por meio das instalações da SWIFT estão sujeitas às normas e regulamentos da SWIFT em vigor, incluindo as normas de associação. O Cliente se responsabiliza por se familiarizar e estar em conformidade com os padrões das mensagens SWIFT.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission *Assinatura digital / eletrônica Métodos de autenticação para envio de documentos eletrônicos*	
Digital Signature *Certificados digitais*	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. Um tipo de assinatura eletrônica que utiliza o certificado digital para validar a autenticidade e a integridade de uma assinatura, mensagem, software ou documento digital.

Electronic Signature *Assinatura eletrônica*	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. *Um símbolo eletrônico anexado a um contrato ou outro instrumento, exclusivo e usado por uma pessoa com a intenção de assinar. As assinaturas eletrônicas podem ser criadas na forma de palavras, letras, numerais, símbolos, clique em um botão em um site, upload de fac-símile ou digitalização de uma assinatura física, assinatura em uma tela de toque ou concordância com quaisquer termos e condições por meios eletrônicos. Criado sob o controle exclusivo da pessoa que o utiliza, é logicamente anexado ou associado a uma mensagem de dados, capaz de identificar a pessoa que consente com a mensagem de dados e certificar o consentimento da pessoa. Essa assinatura eletrônica é submetida ao Banco por meio dos canais eletrônicos do Banco e em conformidade com os Métodos de Autenticação associados descritos acima.*

Manual Initiated Funds Transfer (MIFT) Authentication Method *Transferência de fundos iniciada manualmente (MIFT) Métodos de autenticação*	
MIFT Authentication *Autenticação 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. *A Transferência de fundos iniciada manualmente (MIFT - Manual Initiated Funds Transfer), incluindo emendas, retiradas ou cancelamentos de instruções manuais anteriores, pode ser feita por fax ou carta ou por meio de upload ao CitDuirct CitiDirect. Nem todos os formulários são aceitos em todos os países. Iniciadores são pessoas designadas pelo Cliente que estão autorizadas a iniciar transações de acordo com restrições, se houver, e são identificadas pelo Cliente. Confirmadores são pessoas designadas pelo Cliente para as quais o Banco pode ligar novamente, a seu critério, para confirmar instruções iniciadas manualmente para transferências de fundos.* 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. *Em alguns países, os números de telefone celular não são aceitos como números de retorno de chamada. Detalhes adicionais são fornecidos no Guia do Usuário da Gestão de Caixa do País, Autorização de Transação Manual Global ou Formulário de Nomeação Universal aplicável. O MIFT deve ser usado pelo Cliente como um método de contingência para comunicar instruções ao Banco.*

Mail, Fax, Email and Messenger Authentication Methods *Correio, fax, e-mail e mensageiro Métodos de autenticação*	
Seal Image Verification *Verificação da imagem*	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. *As correspondências recebidas pelo Banco via fax, correio, e-mail ou mensageiro, excluindo as solicitações MIFT, são verificadas e agrupadas com o devido cuidado, com base na imagem contida no documento de autorização do Cliente ou documento semelhante fornecido ao Banco.*
Signature Verification *Verificação da assinatura*	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. *As correspondências recebidas pelo Banco via fax, correio, e-mail ou mensageiro, excluindo as solicitações MIFT, são assinaturas verificadas com base na informação contida no documento de autorização do Cliente ou documento semelhante fornecido ao Banco.*
Secure PDF *PDF Seguro*	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. *Os e-mails criptografados são entregues em uma caixa de correio comum como documentos PDF que podem ser abertos digitando uma senha privada. O corpo da mensagem e todos os arquivos anexados são criptografados. Uma senha privada pode ser configurada após o recebimento do primeiro e-mail seguro recebido.*
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. *O MTLS (Mandatory Transport Layer Security) cria o que seria uma conexão de e-mail privada e segura entre o Banco e o Cliente. E-mails transmitidos por este canal são enviados via Internet por um túnel TLS criptografado criado pela conexão.*

Phone Authentication Methods *Telefone Métodos de autenticação*	
PIN PIN	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *Os clientes que entram em contato com o Banco por telefone devem digitar um PIN para validar o acesso autorizado.*
Verification Questions *Perguntas para verificação*	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. *Os clientes que entram em contato com o Banco por telefone são solicitados pelos representantes de serviço do Banco a fornecerem respostas verbais corretas às perguntas para verificação a fim de validar o acesso autorizado.*

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

A disponibilidade dos Métodos de Autenticação descritos abaixo varia de acordo com os mercados locais.

3. Customer Responsibilities
Responsabilidades do Cliente

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.

Identificação de usuários autorizados: O Cliente é responsável por identificar: (i) todos os indivíduos que atuam na(s) Conta(s) em nome do Cliente em nível de entidade para todos os Serviços e canais de conectividade, e (ii) cada pessoa que atua em nome do Cliente está devidamente autorizada pelo Cliente a agir na Conta do Cliente.

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.

O Cliente é responsável por atribuir e monitorar quaisquer limites de transação atribuídos ao Cliente e / ou seus usuários e garantir que esses limites (a) não excedam os limites exigidos pelas políticas internas do Cliente e outras autoridades e documentos constitutivos, como o Conselho de Administração do Cliente. As resoluções do diretor, mandatos do banco, procuração ou documento equivalente, e (b) são refletidas adequadamente em todos os canais de conectividade e direitos do usuário.

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.

Certas jurisdições podem exigir que os indivíduos (e suas Credenciais correspondentes) sejam identificados pelo Banco em conformidade com os requisitos aplicáveis da legislação de combate à lavagem de dinheiro (AML) antes de conceder acesso para realizar certas funções. Entre em contato com ou representante de atendimento ao cliente ou visite o CitiDirect BE website para mais informações.

3.4 Safeguarding of Authentication Methods

Proteção dos Métodos de Autenticação

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.

O Cliente é responsável por proteger os Métodos de Autenticação e Credenciais com o mais alto padrão de cuidado e diligência, além de garantir que o acesso e a distribuição das Credenciais sejam limitados apenas às pessoas autorizadas pelo Cliente.

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.

Comunicações enviadas por terceiros: Quando o Cliente estiver usando uma Credencial para identificar e autenticar as suas Comunicações como originárias de uma entidade legal, o Cliente é responsável por exercer controle total sobre o uso de tais Credenciais ao enviar Comunicações ao Banco, incluindo quando essas Comunicações são enviadas por aplicativos e / ou sistemas gerenciados por terceiros em nome do Cliente. Em todos os casos, o Banco (a) considerará qualquer Comunicação que receba por meio de um canal de conectividade eletrônica que tenha sido recebida pelo Banco em conformidade com estes Procedimentos de Segurança como tendo sido devidamente autenticados como tendo se originado do Cliente, como uma Comunicação instruída pelo Cliente e (b) pode agir de acordo com qualquer Comunicação que receba em nome do Cliente, em conformidade com estes Procedimentos de Segurança.

4. Data Integrity and Secured Communications
C. Integridade dos dados e comunicações seguras

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.

O Cliente transmitirá dados e trocará Comunicações com o Banco via Internet, correio, e-mail e/ou fax, que, de acordo com o entendimento do Cliente, não são (i) necessariamente sistemas de comunicação e de entrega seguros e (ii) sob o controle do Banco.

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.

O Banco utiliza métodos de criptografia líderes do setor (conforme determinado pelo Banco), o que ajuda a garantir que a informação seja mantida em sigilo e que não seja alterada durante o trânsito eletrônico.

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.

Se o Cliente suspeitar ou tomar conhecimento de uma falha técnica ou qualquer acesso ou uso indevido ou potencialmente fraudulento dos Serviços ou canais de conectividade ou Métodos de Autenticação do Banco por qualquer pessoa (seja uma pessoa autorizada ou não), o Cliente deverá notificar prontamente o Banco de tal ocorrência. No caso de acesso ou uso indevido ou potencialmente fraudulento por parte de uma pessoa autorizada, o Cliente deve tomar medidas imediatas para cancelar o acesso e o uso desses Serviços ou canais de conectividade do Banco.

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.

Se o Cliente usa software de formatação ou criptografia de arquivos (seja fornecido pelo Banco ou por um terceiro) para suporte à formatação e ao reconhecimento de dados e instruções do Cliente e atua sobre as comunicações com o Banco, então o Cliente usará esse software apenas para os fins para os quais ele foi instalado.

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.

O Cliente aceita que o Banco pode suspender ou negar o acesso dos usuários aos Serviços que exijam o uso de Credenciais (i) em caso de suspeita de uso não autorizado ou fraudulento das Credenciais e / ou (ii) para proteger os Serviços ou Credenciais.

5. Security Manager and Related Functions
Usuário Master e funções relacionadas

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:

Para aplicativos acessíveis no CitiDirect BE (com exceção dos Certificados Pessoais discutidos abaixo), o Banco exige que o Cliente estabeleça uma função "Usuário Master". Os Usuário Master são responsáveis por:

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);

Estabelecer e manter o acesso e os direitos dos usuários (incluindo os próprios Usuário Master), incluindo atividades como: (a) criação, exclusão ou modificação de Perfis de Usuário (incluindo Perfis do Usuário Master) e atribuição de direitos (observe que o nome do usuário deve estar alinhado aos documentos de identificação comprobatórios); (b) criação de perfis de acesso que definem as funções e dados disponíveis para vários usuários; (c) ativação e desativação das credenciais de login do usuário; e (d) atribuição de limites de transação (observe que esses limites não são monitorados nem validados pelo Banco e o Cliente deve monitorar esses limites para garantir que estejam em conformidade com as políticas e requisitos internos do Cliente, incluindo, entre outros, aqueles estabelecidos pelo Conselho de Administração do Cliente; ou equivalente);

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;

Criação e modificação de lançamentos em bibliotecas mantidas pelo Cliente (tais como pagamentos pré-formatados e bibliotecas de beneficiários) e autorização de outros usuários a fazer o mesmo;

5.3 Modifying payment authorization flows;

Modificação dos fluxos de autorização de pagamento;

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

Alocação de credenciais de senha dinâmicas ou outras credenciais de acesso ao sistema ou senhas aos usuários do Cliente; e

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

Notificação ao Banco se houver algum motivo para suspeitar que a segurança foi comprometida.

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.

Observação: As funções e responsabilidades do Usuário Master podem variar ou não serem aplicáveis em determinados mercados devido a requisitos regulatórios e / ou recursos operacionais. Nesses mercados, o Banco pode exigir documentação adicional e outras informações do Cliente para desempenhar as funções do Usuário Master em nome do Cliente.

6. Use of CitiDirect BE by Security Managers
Uso do CitiDirect BE por Usuário Master

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.

O Banco exige dois (2) indivíduos separados para registrar e autorizar instruções; portanto, exige-se um mínimo de dois Usuário Master. Quaisquer dois Usuário Master, atuando em conjunto, podem dar instruções e/ou confirmações através dos canais de conectividade em relação a qualquer função do Usuário Master ou em conexão com a facilitação de nossa comunicação. Quaisquer comunicações desse tipo, quando autorizadas por dois Usuário Master, serão aceitas e processadas pelo Banco e consideradas como tendo sido concedidas pelo Cliente. O Banco recomenda a designação de pelo menos três Usuário Master para garantir o backup adequado. O Cliente deve designar seus Usuário Master no Formulário de Admissão de Canais TTS. Um Usuário Master do Cliente também pode atuar como Usuário Master para uma entidade terceirizada (por exemplo, uma afiliada do Cliente) e exercer todos os direitos relacionados a ela (incluindo, entre eles, a nomeação de usuários para a(s) Conta(s) da entidade terceirizada), sem qualquer outra designação, caso essa entidade terceirizada assine um formulário de Autorização de Acesso Universal (ou qualquer outra forma de autorização aceitável pelo Banco), que concede ao Cliente o acesso a sua(s) conta(s). Isso se aplica somente em relação à(s) Conta(s) abrangida(s) pelo formulário relevante.

7. Use of CitiDirect BE by Security Officers (For Personal Certificates only)
Uso do CitiDirect BE por Agentes de Segurança (somente para Certificados Pessoais)

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.

O Banco exige dois (2) indivíduos separados para gerenciar certificados digitais atribuídos a indivíduos ("Certificados Pessoais"). Portanto, são necessários dois Agentes de Segurança para atribuir e remover Certificados Pessoais aos usuários, com o objetivo de autenticar e autorizar as Comunicações nos canais de conectividade. O Banco recomenda a designação de pelo menos três Agentes de Segurança para garantir o backup adequado. Quaisquer Comunicações autorizadas pelos Certificados Pessoais serão aceitas e processadas pelo Banco e como tendo sido concedida pelo Cliente.

This document is registered with the: (i) 1st Registry Office of Title Deeds and Documents of the City of São Paulo, under microfilm no. 3.698.065, registered under margin no. 3.364.930; (ii) 3rd Registry Office of Title Deeds and Documents of the City of São Paulo, under the microfilm no 9.083.827, registered under margin no. 277.846, 303.986, 317.503, 1.471.007, 1.544.268, 3.974.532, 3.974.533, 3.974.534, 3.974.535, 6.426.885, 6.426.886, 6.563.691, 6.563.692, 6.563.693, 7.927.346, 8.137.531, 8.158.356, 8.273.962, 8.306.516, 8.306.517, 8.306.518, 8.306.519, 8.306.520, 8.306.521, 8.306.522, 8.342.781, 8.513.372, 8.935.827, 9.005.238, 9.011.095, 9.021.173, 9.023.969, 9.041.826, 9.050.545, 9.050.570 and 9.067.965; and (iii) 6th Office of the Recorder of Deeds of the City of São Paulo, State of São Paulo under the microfilm No 1.921.581, registered under margin nº 1.435.407, 1.592.375, 1.592.376, 1.664.522, 1.674.836, 1.713.856, 1.752.326, 1.760.789, 1.761.376, 1.803.162, 1.813.155, 1.829.064, 1.834.940, 1.846.532, 1.853.500, 1.864.025, 1.866.501, 1.882.273, 1.892.037, 1.892.050, 1.910.288 and 20.403.844.

Este documento está registrado no: (i) 1º Cartório de Registro e Títulos e Documentos da Cidade de São Paulo, sob o nº. 3.698.065, a margem de 3.364.930; (ii) 3º Cartório de Registro e Títulos e Documentos da Cidade de São Paulo, sob o microfilme nº 9.083.827Averbado sob a margem nº 277.846, 303.986, 317.503, 1.471.007, 1.544.268, 3.974.532, 3.974.533, 3.974.534, 3.974.535, 6.426.885, 6.426.886, 6.563.691, 6.563.692, 6.563.693, 7.927.346, 8.137.531, 8.158.356, 8.273.962, 8.306.516, 8.306.517, 8.306.518, 8.306.519, 8.306.520, 8.306.521, 8.306.522, 8.342.781, 8.513.372, 8.935.827, 9.005.238, 9.011.095, 9.021.173, 9.023.969, 9.041.826, 9.050.545, 9.050.570 e 9.067.965; e (iii) 6º Registro de Títulos e Documentos da Cidade de São Paulo, Estado de São Paulo, sob o microfilme No. 1.921.581, averbado sob a margem nº 1.435.407, 1.592.375, 1.592.376, 1.664.522, 1.674.836, 1.713.856, 1.752.326, 1.760.789, 1.761.376, 1.803.162, 1.813.155, 1.829.064, 1.834.940, 1.846.532, 1.853.500, 1.864.025, 1.866.501, 1.882.273, 1.892.037, 1.892.050, 1.910.288 e 20.403.844.

SAC Citi 0800 979 2484 - Customer Service for Complaints, Cancellation of Product and Services and Information.
SAC Citi 0800 979 2484 - Serviço de Apoio ao Cliente para Reclamação, Cancelamento de Produtos e Serviços e Informações.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions