Security Procedures
Procédures de sécurité

1. Introduction
Introduction

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).

Ces « procédures de sécurité », tel qu'il y est fait mention dans la section « Communications » des conditions générales de compte-principal et de service (« MAST ») (ou autres conditions générales de compte applicable), sont conçues pour authentifier la connexion du Client aux canaux de connectivité de la Banque et pour vérifier l'origine des communications entre la Banque et le Client dans le cadre des services ou des canaux de connectivité suivants (dont la disponibilité peut varier selon les marchés locaux).

- CitiDirect® (including WorldLink®)
  CitiDirect® (y compris WorldLink®)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  SWIFT (Société de télécommunications financières interbancaires mondiales)
- Manual Initiated Funds Transfer ("MIFT")
  Virement manuel de fonds (« MIFT »)
- Interactive Voice Response ("IVR")
  Réponse vocale interactive (« IVR »)
- Email/Fax/Mail/Messenger/Phone with the Bank
  Courriel, télécopie, courrier, messagerie, appel téléphonique avec la banque
- Other local electronic connectivity channels
  Autres canaux de connectivité électronique locale

These Security Procedures are to be read together with the MAST and may be updated and advised to the Customer from time-to-time by electronic or other means, including but not limited to posting updates to the Security Procedures on CitiDirect. Unless otherwise provided by law, Customer's continued use of any of the above noted Services or connectivity channels after being advised of updated Security Procedures shall constitute Customer's acceptance of such updated Security Procedures. These Security Procedures cover the following:

Ces procédures de sécurité doivent être lues conjointement avec le MAST et peuvent être occasionnellement mises à jour et communiquées au Client par voie électronique ou autre, notamment à travers la publication de mises à jour des procédures de sécurité sur CitiDirect. Sauf disposition contraire de la loi, l'utilisation continue par le Client de l'un des services ou des canaux de connectivité susmentionnés après avoir été informé de la mise à jour des procédures de sécurité constitue l'acceptation par le Client de ces procédures de sécurité mises à jour. Ces procédures de sécurité couvrent les éléments suivants :

A. Authentication Methods
Les Méthodes d'authentification

B. Customer Responsibilities
Les Responsabilités du Client

C. Data Integrity and Secured Communications
L'Intégrité des données et communications sécurisées

D. Security Manager and Related Functions
Administrateur de la sécurité et fonctions connexes

2. Authentication Methods *Méthodes d'authentification*

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.

Les procédures de sécurité comprennent certaines méthodes d'authentification sécurisées (« méthodes d'authentification ») qui sont utilisées pour identifier et vérifier de manière unique l'autorité du Client ou de l'un de ses utilisateurs autorisés par le Client. L'identification et la vérification ont généralement lieu au moyen d'un mécanisme ou d'une combinaison de mécanismes comme un identifiant et un mot de passe, des certificats numériques, la biométrie, des jetons de sécurité (déployés par le biais du matériel ou du logiciel), la vérification de scellés et signatures ou des dispositifs associés aux méthodes d'authentification (collectivement appelés les « identifiants »). Les méthodes d'authentification et les identifiants associés permettent à la Banque de vérifier l'origine des communications qu'elle reçoit.

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.

De plus amples informations concernant les méthodes d'authentification pour l'accès aux services ou aux canaux de connectivité sont disponibles sur la page d'aide à la connexion du site Web de CitiDirect. Le Client peut à tout moment sélectionner une des méthodes d'authentification disponibles. Lors de la mise en œuvre des services ou des canaux de connectivité, la Banque peut définir une méthode d'authentification par défaut, que le Client peut modifier à tout moment pour choisir une autre méthode d'authentification disponible.

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

Les méthodes d'authentification suivantes sont disponibles pour accéder aux services ou aux canaux de connectivité :

CitiDirect Authentication Methods *CitiDirect Méthodes d'authentification*	
Biometrics *Biométrie*	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. *Une méthode d'authentification numérique qui utilise les caractéristiques physiques uniques d'un utilisateur (comme une empreinte digitale et une reconnaissance faciale), une technologie biométrique intégrée sur le dispositif mobile de l'utilisateur et des techniques cryptographiques pour accéder à CitiDirect. Les données relatives aux caractéristiques physiques ne sont pas transférées à la Banque lorsque l'utilisateur choisit cette méthode d'authentification.*
Mobile Token (non-application based) *Jeton mobile* *sans application dédiée)*	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. *Méthode d'authentification mobile numérique sans application (par exemple, un jeton mobile sans application) utilisant des clés cryptographiques et une authentification biométrique (empreinte digitale ou reconnaissance faciale) pour associer l'appareil mobile d'un utilisateur à son compte CitiDirect via son navigateur mobile. Lorsque l'utilisateur choisit ce mode d'authentification, aucune donnée biométrique n'est transmise à la Banque lorsque l'utilisateur opte pour ce mode d'authentification. Cette méthode facilite l'authentification multifacteur en vérifiant l'identité de l'utilisateur au moyen de son appareil mobile enregistré.*
Challenge Response Token *Jeton de réponse de vérification*	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. *Soit (i) un jeton logiciel basé sur une application mobile (par exemple MobilePASS), soit (ii) un jeton physique (par exemple SafeWord Card, Vasco), qui, dans chacun des cas, est utilisé pour générer un mot de passe dynamique après authentification à l'aide d'un code secret (par exemple un code secret à 4 chiffres). Lors de l'accès à CitiDirect, le système génère une vérification et un code de réponse est produit par le jeton utilisé et saisi dans le système. Cette méthode d'authentification, lorsqu'elle est combinée à un mot de passe sécurisé, produit une authentification multifactorielle.*
One-Time Password Token *Jeton à mot de passe unique*	Either (i) a mobile application 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. *Soit (i) un jeton logiciel basé sur une application mobile (par exemple MobilePASS), soit (ii) un jeton physique (par exemple SafeWord Card, Vasco), qui est utilisé pour générer un mot de passe dynamique après authentification par un code secret (par exemple un code secret à 4 chiffres). Ce mot de passe dynamique est saisi dans le système pour en obtenir l'accès.*

CitiDirect Authentication Methods ***CitiDirect Méthodes d'authentification***	
Secure Password *Mot de passe sécurisé*	A user enters his or her secure password to access the system. A secure password typically limits a user's capabilities on the system, for example, by only permitting that certain information be viewed by the user. This authentication method, when combined with a challenge response token results in multifactor authentication. *Un utilisateur entre son mot de passe sécurisé pour accéder au système. Un mot de passe sécurisé limite généralement les capacités d'un utilisateur sur le système, par exemple, en ne permettant à ce dernier que la consultation de certaines informations. Cette méthode d'authentification, lorsqu'elle est combinée à un jeton de réponse de vérification, produit une authentification multifactorielle.*
SMS One-Time Code *Code SMS à usage unique*	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. *Un mot de passe dynamique délivré aux utilisateurs par SMS, que l'utilisateur saisit ensuite avec un mot de passe sécurisé pour accéder au système.*
Voice One-Time Code *Code vocal unique*	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. *Un mot de passe dynamique délivré aux utilisateurs par un appel vocal automatisé, que l'utilisateur saisit ensuite avec un mot de passe sécurisé pour accéder au système.*
Digital Certificates *Certificats numériques*	A digital certificate is an electronic identification issued by an approved certificate authority for authentication and authorization. Digital certificates may be attributed to corporate legal entities ("Corporate Seals") or individuals ("Personal Certificates"). The Customer is responsible for properly verifying the identity of all users of Personal Certificates acting on behalf of the Customer in accordance with local law. The Bank and the Customer are required to use digital certificates provided by authorized persons, to ensure all Communications exchanged via a public internet connection or an otherwise unsecure internet connection are fully encrypted and protected. *Un certificat numérique est une identification électronique délivrée par une autorité de certification agréée à des fins d'authentification et d'autorisation. Les certificats numériques peuvent être attribués à des personnes morales (« Corporate Seals ») ou à des personnes physiques (« Personal Certificates »). Le Client est en charge de la verification de l'identité de tous les utilisateurs de certificats personnels agissant en son nom, conformément à la législation locale.* *La Banque et le Client sont tenus d'utiliser des certificats numériques fournis par des personnes autorisées afin de garantir que toutes les communications échangées par le biais d'une connexion Internet publique ou d'une connexion Internet non sécurisée sont entièrement cryptées et protégées.*

CitiConnect for Files Authentication Methods *CitiConnect pour fichiers Méthodes d'authentification*	
Digital Certificates *Certificats numériques*	See description above. *Voir la définition ci-dessus.*

CitiConnect for Files Authentication Methods *CitiConnect pour fichiers Méthodes d'authentification*	
IP Address Whitelist When Using CitiConnect *Liste blanche des adresses IP lors de l'utilisation de 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. *Certaines communications Internet que reçoit la Banque, par exemple par le biais d'un réseau privé virtuel (VPN), peuvent également reposer sur l'échange d'informations entre les parties au moyen d'adresses IP (Internet Protocol) convenues au préalable. La Banque n'accepte que les communications provenant de l'adresse IP désignée du Client, et vice versa, et elle ne transmet les communications qu'à l'adresse IP désignée du Client, et vice versa. Utilisée en conjonction avec la méthode de certificat numérique décrite ci-dessus.*

CitiConnect API Authentication Methods ***API CitiConnect Méthodes d'authentification***	
Digital Certificates *Certificats numériques*	See description above. *Voir la définition ci-dessus.*
IP Address Whitelist When Using CitiConnect *Liste blanche des adresses IP lors de l'utilisation de CitiConnect*	See description above. *Voir la définition ci-dessus.*

CitiConnect for SWIFT Authentication Methods ***CitiConnect pour SWIFT Méthodes d'authentification***	
Digital Certificates *Certificats numériques*	See description above. Can be used in conjunction with SWIFT Authentication method below. *Voir la définition ci-dessus. Peut être utilisé en conjonction avec la méthode d'authentification SWIFT décrite ci-dessous.*

CitiConnect for SWIFT Authentication Methods *CitiConnect pour SWIFT Méthodes d'authentification*	
SWIFT Authentication *Authentification SWIFT*	Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWiFT's Contractual Documentation (as amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications. The Bank is not responsible for any errors or delays in the SWIFT system. The Customer is responsible for providing communications to the Bank in the format and type required and specified by SWIFT. Transmissions and Communications sent or received via SWIFT facilities are subject to SWIFT rules and regulations in effect, including membership rules. The Customer is responsible for being familiar with and conforming to SWIFT messaging standards. *Les communications envoyées entre la Banque et le Client par le biais du réseau SWIFT, notamment les informations sur les comptes, les ordres de paiement et les instructions de modification ou d'annulation de ces ordres, seront authentifiées au moyen des procédures définies dans la documentation contractuelle SWIFT (telle qu'elle peut être occasionnellement modifiée ou complétée), qui comprend entre autres ses conditions générales et la description du service FIN ou tel qu'indiqué dans d'autres conditions générales qui peuvent être établies par SWIFT. La Banque n'est pas tenue de faire autre chose que ce qui est contenu dans les procédures SWIFT pour établir l'expéditeur et l'authenticité de ces communications.* *La Banque n'est pas administrateur des erreurs ou des retards dans le système SWIFT. Le Client est tenu de fournir à la Banque des communications dans le format et le type requis et spécifié par SWIFT.* *Les transmissions et les communications envoyées ou reçues par l'intermédiaire des installations SWIFT sont soumises aux règles et règlements SWIFT en vigueur, y compris les règles d'adhésion. Le Client est tenu de se familiariser et de se conformer aux normes de messagerie SWIFT.*

SWIFT Authentication Method ***SWIFT Méthode d'authentification***	
SWIFT Authentication (Direct Connection for Financial Institutions) *Authentification SWIFT (connexion directe pour les établissements financiers)*	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. *Les communications envoyées entre la Banque et le Client par le biais du réseau SWIFT, notamment les informations sur les comptes, les ordres de paiement et les instructions de modification ou d'annulation de ces ordres, seront authentifiées au moyen des procédures définies dans la documentation contractuelle SWIFT (telle qu'elle peut être occasionnellement modifiée ou complétée), qui comprend entre autres ses conditions générales et la description du service FIN ou tel qu'indiqué dans d'autres conditions générales qui peuvent être établies par SWIFT. La Banque n'est pas tenue de faire autre chose que ce qui est contenu dans les procédures SWIFT pour établir l'expéditeur et l'authenticité de ces communications.* *La Banque n'est pas administrateur des erreurs ou des retards dans le système SWIFT. Le Client est tenu de fournir à la Banque des communications dans le format et le type requis et spécifié par SWIFT.* *Les transmissions et les communications envoyées ou reçues par l'intermédiaire des installations SWIFT sont soumises aux règles et règlements SWIFT en vigueur, y compris les règles d'adhésion. Le Client est tenu de se familiariser et de se conformer aux normes de messagerie SWIFT.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Signature numérique/électronique Méthodes d'authentification pour la remise de documents électroniques***	
Digital Signature *Signature numérique*	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. *Un type de signature électronique qui utilise des certificats numériques pour valider l'authenticité et l'intégrité d'une signature, d'un message, d'un logiciel ou d'un document numérique.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Signature numérique/électronique Méthodes d'authentification pour la remise de documents électroniques***	
Electronic Signature *Signature électronique*	An electronic symbol attached to a contract or other record, unique to and used by a person with an intent to sign. Electronic signatures can be established in the form of words, letters, numerals, symbols, click of a button on a website, upload of facsimile or scan of a physical signature, signing on a touchscreen, or agreeing to any terms and conditions by electronic means. Created under the sole control of the person using it, it is logically attached to or associated with a data message capable of identifying the person who consents to the data message and certifying the person's consent. Such Electronic Signature would be submitted to the Bank through the Bank's electronic channels and in compliance with the associated Authentication Methods described above. *Un symbole électronique attaché à un contrat ou à un autre document, unique à une personne et utilisé par celle-ci dans l'intention de signer. Les signatures électroniques peuvent être établies sous forme de mots, de lettres, de chiffres, de symboles, d'un clic sur un bouton sur un site Web, du téléchargement d'un fac-similé ou de la lecture d'une signature physique, de la signature sur un écran tactile ou de l'acceptation de conditions générales par des moyens électroniques. Créée sous le contrôle exclusif de la personne qui l'utilise, elle est rattachée ou associée de manière logique à un message de données, elle permet d'identifier la personne qui consent au message de données et elle certifie le consentement de cette personne. Cette signature électronique est soumise à la Banque par les canaux électroniques de la Banque et conformément aux méthodes d'authentification associées décrites ci-dessus.*

Manual Initiated Funds Transfer (MIFT) Authentication Method ***Virement manuel de fonds (MIFT) Méthode d'authentification***	
MIFT Authentication *Authentification MIFT*	Manually Initiated Funds Transfer (MIFT), including amendments, recalls, or cancellations 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 communication instructions to the Bank. *Les virements manuels de fonds (MIFT), y compris les modifications, les rappels ou les annulations d'instructions manuelles antérieures, peuvent être effectués par télécopie ou par lettre, ou être téléchargés sur CitiDirect. Tous les formulaires ne sont pas pris en charge dans tous les pays. Les initiateurs sont des personnes désignées par le Client qui sont autorisées à initier des opérations conformément aux restrictions qui sont, le cas échéant, identifiées par le Client. Les personnes en charge de la confirmation sont des personnes désignées par le Client que la Banque peut rappeler, à sa discrétion, pour confirmer les instructions de virement de fonds initiées manuellement.* *Dans certains pays, les numéros de téléphone portable ne sont pas acceptés comme numéros de rappel. De plus amples détails sont fournis dans le guide de l'utilisateur de la gestion de trésorerie du pays concerné, dans l'autorisation manuelle globale des opérations ou dans le formulaire de nomination universel. La méthode MIFT doit être utilisé par le Client comme méthode de secours pour communiquer des instructions à la Banque.*

Mail, Fax, Email and Messenger Authentication Methods ***Courrier, fax, courriel et service de messagerie Méthodes d'authentification***	
Seal Image Verification *Vérification des images de scellés*	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. *La correspondance que reçoit la Banque par fax, courrier, courriel ou service de messagerie, à l'exclusion des demandes MIFT, est vérifiée et rassemblée avec un contrôle rigoureux sur la base de l'image des scellés figurant dans le document d'autorisation du Client ou dans un document similaire fourni à la Banque.*
Signature Verification *Vérification de la signature*	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. *La correspondance que reçoit la Banque par fax, courrier, courriel ou service de messagerie, à l'exclusion des demandes MIFT, fait l'objet d'une vérification de signature sur la base des informations contenues dans le document d'autorisation du Client ou dans un document similaire fourni à la Banque.*

Mail, Fax, Email and Messenger Authentication Methods ***Courrier, fax, courriel et service de messagerie Méthodes d'authentification***	
Secure PDF *PDF sécurisé*	Encrypted emails are delivered to a regular mailbox as PDF documents that are opened by entering a private password. Both the message and body and any attached files are encrypted. A private password can be set up upon receipt of the first secure email received. *Les courriers électroniques cryptés sont envoyés dans une boîte aux lettres ordinaire sous forme de documents PDF qui sont ouverts en saisissant un mot de passe privé. Le corps du message et les fichiers joints sont tous deux cryptés. Un mot de passe privé peut être configuré à la réception du premier courriel sécurisé reçu.*
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. *La sécurisation MTLS crée ce qui serait une connexion de courrier électronique privée et sécurisée entre la Banque et le Client. Les courriers électroniques transmis par ce canal sont envoyés sur Internet par un tunnel TLS crypté créé par la connexion.*

Phone Authentication Methods ***Téléphone Méthodes d'authentification***	
PIN *Code secret*	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *Les clients qui contactent la Banque par téléphone sont invités à saisir un code secret pour valider l'accès autorisé.*
Verification Questions *Questions de vérification*	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. *Les Clients qui contactent la Banque par téléphone sont invités par les représentants du service de la Banque à fournir des réponses verbales correctes aux questions de vérification afin de valider l'accès autorisé.*

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

La disponibilité des méthodes d'authentification décrites ci-dessus varie en fonction des marchés locaux.

3. Customer Responsibilities
Responsabilités du Client

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.

Identification des utilisateurs autorisés – Le Client est tenu d'identifier : (i) toutes les personnes agissant sur le(s) compte(s) au nom du Client au niveau de l'entité pour tous les services et canaux de connectivité, et (ii) chaque personne agissant au nom du Client et dûment autorisée par ce dernier à agir sur son compte.

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.

Le Client est chargé d'attribuer et de suivre toutes les limites d'opérations qui lui sont attribuées ou à ses utilisateurs et de s'assurer que ces limites (a) ne dépassent pas les limites qu'imposent les politiques internes du Client et autres documents d'autorité et constitutifs tels que les résolutions du conseil d'administration du Client, les mandats bancaires, les procurations ou documents équivalents, et (b) sont correctement formulées sur tous les canaux de connectivité et les droits des utilisateurs.

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.

Certaines juridictions peuvent exiger que la Banque identifie les personnes (et leurs identifiants correspondants) conformément aux exigences de la législation LBC applicable avant de leur accorder l'accès à certaines fonctions. Veuillez contacter votre représentant du service clientèle ou consulter le site Web de CitiDirect pour de plus amples informations.

3.4 Safeguarding of Authentication Methods
Sauvegarde des méthodes d'authentification

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.

Le Client est chargé de sauvegarder les méthodes d'authentification et les identifiants avec le plus grand soin et la plus grande diligence, et de s'assurer que l'accès aux identifiants et leur distribution se limitent aux personnes autorisées par le Client.

Communications envoyées par une tierce partie – Lorsque le Client utilise un identifiant pour identifier et authentifier la provenance de ses communications en tant que personne morale, il est administrateur du contrôle total sur l'utilisation de ces identifiants lors de l'envoi de communications à la Banque, y compris lorsque ces communications sont envoyées par des applications ou des systèmes qui sont gérés par un tiers au nom du Client. Quelles que soient les circonstances, la Banque (a) considérera que toute communication qu'elle reçoit par un canal de connectivité électronique conformément aux présentes procédures de sécurité et dûment authentifiée comme provenant du Client est une communication requise par le Client et (b) pourra donner suite à toute communication qu'elle reçoit pour le compte du Client conformément aux présentes procédures de sécurité.

4. Data Integrity and Secured Communications
Intégrité des données et communications sécurisées

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.

Le Client transmettra des données à la Banque et échangera des communications avec elle via Internet, courrier, courriel et/ou fax. Le Client reconnaît que ces moyens de communication et de transmission ne sont (i) pas nécessairement sécurisés et (ii) pas sous le contrôle de la Banque. Le Client comprend également que si ses utilisateurs ont accès à Open Banking et/ou à des plateformes tierces similaires en dehors des systèmes Citi, les données du Client peuvent être transmises via ces plateformes tierces, qui ne sont pas sous le contrôle de la Banque.

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.

La Banque utilise des méthodes de cryptage de pointe (déterminées par la Banque), qui contribuent à garantir que les informations restent confidentielles et qu'elles ne sont pas modifiées pendant le transfert électronique.

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.

Si le Client soupçonne ou a connaissance d'une défaillance technique ou de tout accès ou utilisation inapproprié(e) ou potentiellement frauduleux(se) des services de la Banque ou des canaux de connectivité ou méthodes d'authentification par une personne quelconque (autorisée ou non), le Client doit en informer rapidement la Banque. En cas d'accès ou d'utilisation abusive ou potentiellement frauduleuse par une personne autorisée, le Client doit prendre des mesures immédiates pour mettre fin à l'accès et à l'utilisation des services ou des canaux de connectivité de la Banque par cette personne autorisée.

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.

Si le Client utilise un logiciel de formatage ou de cryptage de fichiers (qu'il soit fourni par la Banque ou par un tiers) pour prendre en charge le formatage et la reconnaissance des données et des instructions du Client et s'il donne suite aux communications échangées avec la Banque, le Client utilisera ce logiciel uniquement dans le but pour lequel il a été installé.

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.

Le Client accepte que la Banque puisse suspendre ou refuser l'accès des utilisateurs aux services exigeant l'utilisation d'identifiants (i) s'il existe des soupçons d'utilisation non autorisée ou frauduleuse des identifiants ou (ii) pour sauvegarder les services ou les identifiants.

5. Security Manager and Related Functions *Administrateur de la sécurité et fonctions connexes*

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:

Pour les applications accessibles dans CitiDirect (à l'exception des certificats personnels dont il est question ci-dessous), la Banque demande au Client de mettre en place une fonction de « administrateur de la sécurité ». Les administrateurs de la sécurité sont chargés de :

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);

Établir et tenir à jour l'accès et les droits des utilisateurs (dont ceux des administrateurs de la sécurité eux-mêmes), y compris pour des activités comme (a) créer, supprimer ou modifier les profils des utilisateurs (dont les profils des administrateurs de la sécurité) et leurs droits (il est à noter que le nom de l'utilisateur doit correspondre aux documents d'identification associés), (b) établir des profils d'accès qui définissent les fonctions et les données disponibles pour les utilisateurs individuels, (c) activer et désactiver les identifiants de connexion des utilisateurs et (d) attribuer des limites d'opération (il est à noter que ces limites ne sont ni contrôlées ni validées par la Banque et que le Client doit contrôler ces limites pour s'assurer qu'elles sont conformes aux politiques et exigences internes du Client, y compris, sans toutefois s'y limiter, celles établies par le conseil d'administration du Client ou son équivalent) ;

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;

Créer et modifier les entrées dans les bibliothèques gérées par le Client (comme les paiements préformatés et les bibliothèques des comptes des bénéficiaires) et autoriser d'autres utilisateurs à faire de même ;

5.3 Modifying payment authorization flows;

Modifier les flux d'autorisation de paiement ;

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

Attribuer aux utilisateurs du client des mots de passe dynamiques ou autres identifiants ou mots de passe d'accès au système ;

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

Informer la Banque s'il existe une raison de suspecter que la sécurité a été compromise, et

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

Gérer et acquérir des certificats numériques et autoriser d'autres utilisateurs à faire de même.

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.

Il est à noter que les rôles et responsabilités de l'administrateur de la sécurité peuvent varier ou ne pas être applicables sur certains marchés en raison des exigences réglementaires ou des capacités opérationnelles. Sur ces marchés, la Banque peut exiger du Client des documents et informations supplémentaires pour exercer les fonctions d'administrateur de la sécurité pour le compte du Client.

6. Use of CitiDirect and CitiConnect by Security Managers *Utilisation de CitiDirect et CitiConnect par les responsables de la sécurité*

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.

La Banque exige que deux (2) personnes distinctes saisissent et autorisent les instructions. Par conséquent, un minimum de deux administrateurs de la sécurité est requis. Deux administrateurs de la sécurité, agissant de concert, peuvent donner des instructions ou des confirmations par le biais des canaux de connectivité dans le cadre de toute fonction de administrateur de la sécurité ou en vue de faciliter les communications. Lorsqu'elles sont autorisées par deux administrateurs de la sécurité, ces communications sont acceptées par la Banque, qui y donne suite, et elles sont réputées être données par le Client. La Banque recommande que soient nommés au moins trois administrateurs de la sécurité afin d'assurer un soutien adéquat. Le Client doit désigner ses administrateurs de la sécurité sur le formulaire d'intégration des canaux TTS (TTS Channels Onboarding Form). Un administrateur de la sécurité du Client peut également exercer le rôle de administrateur de la sécurité pour une entité tierce (par exemple, une société affiliée au Client) et exercer tous les droits y afférents (y compris la désignation d'utilisateurs pour le(s) compte(s) de cette entité tierce), sans autre forme de désignation, si cette entité tierce signe un formulaire d'autorisation d'accès universel (ou tout autre formulaire d'autorisation acceptable par la Banque) accordant au Client l'accès à son ou ses comptes. Ceci ne s'applique qu'aux comptes couverts par l'autorisation en question.

7. Use of CitiDirect by Security Officers (For Personal Certificates only) *Utilisation de CitiDirect par les agents de sûreté (pour les certificats personnels uniquement)*

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.

La Banque exige que deux (2) personnes distinctes gèrent les certificats numériques attribués aux personnes (« certificats personnels »). Par conséquent, aux fins d'authentification et d'autorisation des communications sur les canaux de connectivité, deux administrateurs de la sécurité sont nécessaires pour attribuer les certificats personnels aux utilisateurs ou les supprimer. La Banque recommande que soient nommés au moins trois administrateurs de la sécurité afin d'assurer un back up adéquat. Lorsqu'elles sont autorisées par des certificats personnels, les communications sont acceptées par la Banque, qui y donne suite, et elles sont confirmées avoir été Fourmies par le Client.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions