Security Procedures
安全程序

1. Introduction
簡介

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).

本安全程序，如同於帳戶及服務主條款之通訊章節或顧客與本行間所簽署其他適用的帳戶條款及條件所述，用於驗證顧客於本行連結管道之登入及顧客與本行間的通訊，範圍包含以下之服務及連結管道(每個國家之適用範圍依當地市場而有所差異)。

- CitiDirect BE® (including WorldLink®)
  CitiDirect BE® (including WorldLink®)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  人工指示交易
- Interactive Voice Response ("IVR")
  互動語音回應
- Email/Fax/Mail/Messenger/Phone with the Bank
  向本行寄發電子郵件/傳真
- Other local electronic connectivity channels
  當地市場其他電子連結管道

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:

本安全程序應與帳戶及服務主條款一併閱讀，且可能隨時更新，並向顧客以電子或其他方式予以通知，包含但不限於在CitiDirect BE上發布安全程序之更新消息。除法律另有規定外，顧客若於接受本程序之更新通知後，仍繼續使用上述任一服務或連結管道，則視為其接受該等更新之程序。本安全程序包含以下內容：

A. Authentication Methods
   驗證方式

B. Customer Responsibilities
   顧客的角色及職責

C. Data Integrity and Secured Communications
資料的完整性及安全通訊

D. Security Manager and Related Functions
安全控管經理及相關職能

2. Authentication Methods
驗證方式

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.

本程序包括某些安全驗證方式(下稱「驗證方式」),係用於辨識並驗證顧客及/或其任何使用者之權限,通常透過使用者識別碼/密碼組合、數位憑證、生物識別、安全代碼(security tokens)(係透過硬體或軟體建制)、簽章辨識等機制進行驗證(以下合稱「驗證資訊」)。驗證方式及相關之驗證資訊可幫助本行驗證顧客向本行發出之通訊來源。

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.

欲瞭解更多驗證方式,請參考CitiDirect BE®登入幫助頁面,網址 https://portal.citidirect.com/portalservices/forms/LoginHelp.pser. 顧客可隨時選擇欲使用之驗證方式,當本行為顧客進行服務及連結管道之建置時,將設定一種預設之驗證方式,顧客可隨時更改為另一種可適用之驗證方式。

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

下列之驗證方式可用於使用服務及連結管道:

CitiDirect BE Authentication Methods CitiDirect BE 驗證方式	
Biometrics 生物識別	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. 運用使用者的生物特徵進行驗證的方式,如指紋及臉部辨識),使用者需利用內建於行動裝置上的生物辨識工具及密碼技術以存取CitiDirect BE,生物特徵的資料將不會被傳送至本行。
Challenge Response Token 安全問題回應	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) 以手機應用程式為基礎之軟體動態密碼(例如MobilePASS)或 (ii) 實體動態密碼(例如SafeWord卡、Vasco);於上述任一情形,以四位數個人識別碼(PIN)進行驗證後,代碼將用以產生一組動態密碼。於使用CitiDirect BE®時,系統將產生一個驗證碼,而所使用的代碼將產生一組回應密碼,用戶再將其輸入於系統中。

One-Time Password Token 一次性密碼:安全代碼	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. 為 (i) 以手機應用程式為基礎之軟體動態密碼 (例如MobilePASS) 或 (ii) 實體動態密碼 (例如SafeWord卡、Vasco) ; 於上述任一情形,以四位數個人識別碼 (PIN) 進行驗證後,代碼將用以產生一組動態密碼。輸入該動態密碼,以取得使用權。
Secure Password 安全密碼	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. 用戶輸入其安全密碼,以取得系統使用權。安全密碼通常限制用戶於系統內之功能,使用戶可檢視資訊,且不會啟用任何交易功能。
SMS One-Time Code SMS一次性密碼	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. 動態密碼係透過簡訊傳送給顧客後,用戶輸入該組動態密碼及一組安全密碼,以取得系統使用權。
Voice One-Time Code Voice一次性密碼	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. 動態密碼透過自動語音電話傳送給顧客後,用戶輸入該組動態密碼及一組安全密碼,以取得系統使用權。
Digital Certificates 數位憑證	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. 用於驗證之數位憑證,係由一受認可之憑證授權單位核發。數位憑證採用密碼儲存機制及相對應的PIN,且可以由IdenTrust、SWIFT (3SKey) 或已認可之其他供應商所核發。數位憑證可分配給機構法人或個人,顧客應負責驗證所有可代表顧客的使用者之個人憑證,以遵守當地法規。 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. 本行及顧客需利用被授權人員提供之憑證以確保所有透過公開網路或不安全的網路進行的通訊被完整的加密並保護。

CitiConnect for Files Authentication Methods CitiConnect for Files 驗證方式	
Digital Certificates 數位憑證	See description above. 如上所述,請參考CitiDirect BE之驗證方式。
IP Address Whitelist When Using CitiConnect 使用CitiConnect的IP位置	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. 特定的通訊方式,如透過VPN,需要雙方以事前議定之IP位置交換資訊,本行只會接受顧客由特定IP位置發起之通訊,本行也只會將資訊傳輸至客戶所指定的IP位置,反之亦然。IP位置及上述之數位憑證需搭配使用。

CitiConnect API Authentication Methods CitiConnect API 驗證方式	
Digital Certificates 數位憑證	See description above. 如上所述，請參考CitiConnect for Files之驗證方式。
IP Address Whitelist When Using CitiConnect 使用CitiConnect的IP位置	See description above. 如上所述，請參考CitiConnect for Files之驗證方式。

CitiConnect for SWIFT Authentication Methods CitiConnect for SWIFT 驗證方式	
Digital Certificates 數位憑證	See description above. Can be used in conjunction with SWIFT Authentication method below. 如上所述，請參考CitiConnect for Files之驗證方式。可與SWIFT驗證方式配合使用。
SWIFT Authentication SWIFT 驗證	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. 本行與顧客透過SWIFT之通訊，包含但不限於帳戶資訊、付款指示、指示修改及取消等，應與SWIFT契約文件所規定之驗證程序相同（該名詞係由SWIFT所定義之名詞，且得隨時修改或補充）；該契約文件包括但不限於其主條款及條件、FIN服務說明、或SWIFT可能訂定之任何其他條款及條件。本行沒有義務執行任何未規範為SWIFT契約文件中的程序以驗證發送者及通訊。 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. 本行對SWIFT系統中任何錯誤或延遲均不負責。顧客向本行所提供之通訊，須以SWIFT所規範及敘明之格式及型態為之。 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. 任何透過SWIFT的資訊傳輸及通訊應受SWIFT之規章規範，包含會員規範。顧客有責任清楚瞭解並遵守SWIFT的通訊標準。

SWIFT Authentication Method SWIFT 驗證方式	
SWIFT Authentication (Direct Connection for Financial Institutions) SWIFT 驗證 (金融機構直接與SWIFT連線)	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. 本行與顧客透過SWIFT之通訊，包含但不限於帳戶資訊、付款指示、指示修改及取消等，應與SWIFT契約文件所規定之驗證程序相同（該名詞係由SWIFT所定義之名詞，且得隨時修改或補充）；該契約文件包括但不限於其主條款及條件、FIN服務說明、或SWIFT可能訂定之任何其他條款及條件。本行沒有義務執行任何未規範為SWIFT契約文件中的程序以驗證發送者及通訊。 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. 本行對SWIFT系統中任何錯誤或延遲均不負責。顧客向本行所提供之通訊，須以SWIFT所規範及敘明之格式及型態為之。 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. 任何透過SWIFT的資訊傳輸及通訊應受SWIFT之規章規範，包含會員規範。顧客有責任清楚瞭解並遵守SWIFT的通訊標準。

Digital/Electronic Signature Authentication Methods for Electronic Document Submission 數位/電子簽章 驗證電子化之文件繳交	
Digital Signature 數位簽章	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. 運用數位憑證以驗證簽章、訊息、軟體、電子文件的真實性、完整性，為電子簽章的一種。
Electronic Signature 電子簽章	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. 可附加於文件的電子標記，每個簽署者應有其獨特且專屬之簽章。電子簽章可以文字、字母、數字、符號、點擊網頁上之按鈕、實體簽章之傳真或掃描檔、於觸控螢幕上完成之簽章或其他有條款依據之電子方式。此簽章應由使用者獨自掌管，可以邏輯性的方式連結至其資料通訊，並且可用於辨識許可此資料通訊者，並驗證其許可。此電子簽章將透過本行之電子連結管道繳交至本行，並遵照上述之相關驗證方式。

Manual Initiated Funds Transfer (MIFT) Authentication Method 人工指示交易 (MIFT) 驗證方式	
MIFT Authentication 人工指示交易驗證	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. 人工指示交易，包含修改、調取或取消先前指示，可以傳真、信件或是經由CitiDirect傳送指示，但並非所有國家都支援上述之方式。啟動人應為顧客所指派，於顧客設立的限制下，可發起交易指示之人員。確認者為顧客所指派之回撥指定人員，本行可以電話回撥之方式確認由人工發起之匯款指示。在特定國家，手機號碼無法作為回撥號碼，更多細節可查看各國家之現金管理使用手冊、全球人工交易授權書或人員授權文件。 人工交易指示可於偶發事件時，用於傳輸指示予本行。 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. 在特定國家，手機號碼無法作為回撥號碼，更多細節可查看各國家之現金管理使用手冊、全球人工交易授權書或人員授權文件。 人工交易指示可於偶發事件時，用於傳輸指示予本行。

Mail, Fax, Email and Messenger Authentication Methods 信件、傳真、電子郵件和通訊軟體 驗證方式	
Seal Image Verification 印章圖像驗證	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. 本行接收之傳真、信件、電子郵件或通訊軟體之通訊，不包含人工交易指示，應與顧客提供與本行之授權文件或類似之文件上之印章進行謹慎之比對驗證。
Signature Verification 簽樣驗證	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. 本行接收之傳真、信件、電子郵件或通訊軟體之通訊，不包含人工交易指示，應與顧客提供與本行之授權文件或類似之文件上之簽樣進行謹慎之比對驗證。
Secure PDF PDF 加密	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. 含有PDF檔案之加密電子郵件發送至一般電子信箱，需輸入個人密碼方可開啟。電子郵件和所有附件都應該進行加密，個人密碼可於第一次收到加密電子郵件時進行設置。
MTLS 強制性傳輸層安全性通訊協定	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. 強制性傳輸層安全通訊協定(MTLS)為本行及顧客建立一安全、私有的電子郵件連結管道，通過此方式傳輸之電子郵件將透過此加密管道於網際網路上進行傳遞。

Phone Authentication Methods 電話 驗證方式	
PIN PIN	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. 顧客以電話聯繫本行時，將被要求輸入PIN碼以驗證身分。
Verification Questions 安全問題	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. 顧客以電話聯繫本行時，本行之電話專員將要求來電者回答安全問題以驗證身份。

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

驗證方式可依不同市場而有所差異。

3. Customer Responsibilities
顧客的角色與職責

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.

確認被授權的使用者：顧客應負責確認：(i)代表顧客之機構於所有服務及連結管道上使用帳戶之使用者及 (ii) 代表顧客使用帳戶的所有使用者皆得到顧客的正式授權。

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.

顧客應負責分配和管控分配給顧客和/或其使用者的所有交易限制，並確保這些限制 (a) 不超過顧客之內部規範以及其他授權及組成文件，如董事會決議、銀行授權書、授權書及其他相同效力文件之限制 (b) 正確反映在所有連結管道和使用者權限。

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.

部分國家可能規定，於其授予執行部分職能之權限前，個別人員 (及其相對應之驗證資訊) 必須被認定為遵循適用之反洗錢法規範。請聯絡您的花旗代表或於CitiDirect BE平台(website)上獲取更多資訊。

3.4 Safeguarding of Authentication Methods

驗證方式之防護

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.

顧客應針對驗證方式及驗證資訊採取高規格的防護，並確保使用、發送驗證資訊的權限僅限於顧客已授權之人員。

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.

第三方發起之通訊: 如果顧客使用驗證資訊來識別和驗證其法律實體產生之通訊，則顧客有責任於向本行發送通訊時，完全掌控制驗證資訊之使用， 包含由第三方代表顧客管理之應用程式和/或系統發送的通訊。在任何情況下，本行均應 (a) 將其通過電子連接管道接收且已經過適當安全程序驗證為來自顧客的通訊，視為顧客指示的通信，並且 (b) 可以按照本安全程序，依據其收到的顧客指示採取行動。

4. Data Integrity and Secured Communications
資料的完整性及安全通訊

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.

顧客可將資料傳輸給本行，並以其他方式 (使用網際網路、電子郵件及 / 或傳真) 與本行進行通訊往來。顧客應該瞭解上述方式並不一定為安全的通訊及傳輸系統，且非本行可控管。

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.

本行使用領先業界的加密方式 (依本行決定是否採用) ，協助您確保資訊處於保密狀態，且資訊於傳輸過程不會遭變更。

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.

如顧客懷疑或知悉發生技術問題，或任何人 (不論是否為被授權人) 不當存取或使用本行服務、連結管道或驗證方式，顧客應立即向本行通知此一情形。如係為被授權人不當存取或使用，顧客應立即採取行動，解除該人存取及使用本行服務或連結管道之權限。

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.

若顧客使用檔案格式化及加密軟體 (無論係由本行或第三方所提供) ，以協助格式化並辨識顧客資料及指示，並依與本行的通訊行事時，顧客使用該等軟體之目的僅限於其安裝目的。

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.

顧客接受本行可能於特定情況中止或拒絕使用者存取需要使用驗證資訊之服務，如 (i) 有疑似未經授權或盜用驗證資訊的情況和/或 (ii) 基於防護服務及驗證資訊之目的。

5. Security Manager and Related Functions
安全控管經理及相關職能

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:

為使應用程式可於CitiDirect BE®使用(下方討論之個人憑證除外)，本行皆要求顧客建立安全控管經理相關流程。安全控管經理之職責如下：

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);

建立並維護使用者(包括安全控管經理自身)使用權限及應有權利，包括以下行動：(a) 產生、刪除或修改使用者資料(包含安全控管經理之資料)及應有權利(請注意，顧客名稱必須與支持的身分證明文件一致)；(b) 建立使用權限資料，此使用權限資料定義給不同使用者之功能及可得的資訊; (c) 啟用及禁用使用者登入驗證資訊; and (d) 分配交易限額(請注意，這些限額不受本行監控或驗證，顧客應監視這些限額，以確保它們符合顧客的內部規範和要求，包括但不限於由顧客董事會建立之規範等。

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;

於顧客維護之資料庫(例如事先製作格式之付款及受益人資料庫)創設並修改各項目，並授權其他使用者亦可創設並修改項目。

5.3 Modifying payment authorization flows;

修改付款授權流程。

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

將動態密碼驗證資訊或其他系統使用驗證資訊或密碼分配給顧客之使用者。

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

若顧客有理由懷疑使用者安全發生問題時，應通知本行。

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.

請注意：由於各地法規之要求和/或營運狀況不同，安全管控經理的角色和職責可能不適用於特定市場或有所差異。 在這樣的市場中，本行可能會要求顧客提供其他文件和信息，以代表顧客執行安全管控經理之功能。

6. Use of CitiDirect BE by Security Managers
安全控管經理使用CitiDirect BE

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.

本行要求顧客需配置兩名獨立人員輸入並授權指示，因此至少需有兩名安全控管經理。兩名安全控管經理係共同行動，且均能透過與任何安全控管經理之職能或促進通訊相關之連結管道，提供指示及 / 或確認。任何通訊經兩名安全控管經理授權後，本行將接受並予以執行，並視其為來自顧客之指示。本行建議，為確保有充足代理人員，顧客至少應配置三名安全控管經理。顧客應於財金暨貿易金融事業群之網路銀行平台啟用申請書，指定其安全控管經理。在沒有任何其他指定下，若該第三方機構以帳戶使用授權書 (或銀行可以接受的其他授權形式)，授權顧客使用其帳戶，顧客的安全控管經理可以作為第三方機構 (例如，顧客的關聯公司) 的安全控管經理，並行使與之相關的所有權利 (包括為該第三方機構的帳戶指定使用者)。 此情況僅適用於相關授權所涵蓋之帳戶。

7. Use of CitiDirect BE by Security Officers (For Personal Certificates only)
安全控管人員使用CitiDirect BE (僅適用於個人憑證)

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.

本行要求顧客配置兩名人員來管理配置給個人的數位憑證(「個人憑證」)。 因此至少需要兩名安全控管人員進行指派和移除個人憑證，以對連結管道上的通信進行驗證和授權。 本行建議至少指派三名安全控管人員以確保有足夠的後備人員。 經個人憑證授權的通信將被本行接受並採取行動，並視為顧客之指示。

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions