Security Procedures
安全程序

1. Introduction
引言

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).

如客户与银行之间订立的账户和服务主协议 ("账户和服务主协议") (或其他适用的账户条款和条件) 的通讯部分所述，以下安全程序设计用于校验用户登录银行的连接渠道以及与以下服务或连接渠道 (可用性可能因当地市场而异) 相关的银行与客户之间通讯的来源。

- CitiDirect® (including WorldLink®)
  CitiDirect® 网银系统(包括 WorldLink®)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  环球银行同业金融电信协会 ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  人工资金转账 ("MIFT")
- Interactive Voice Response ("IVR")
  交互式语音应答 ("IVR")
- Email/Fax/Mail/Messenger/Phone with the Bank
  和银行往来的电子邮件/传真/信件/信使/电话
- Other local electronic connectivity channels
  其他本地电子连接渠道

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. 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:

本安全程序应与账户和服务主协议一起阅读。本安全程序可能会通过电子或其他方式不时更新并通知给客户，包括但不限于在CitiDirect 网银系统上所发布的对安全程序的更新。除非法律另有规定，客户在收到更新安全程序的通知后，如继续使用上述任何服务或连接渠道，则表示客户已接受该等更新的安全程序。本安全程序涵盖以下内容:

A. Authentication Methods
认证方式

B. Customer Responsibilities
客户责任

C. Data Integrity and Secured Communications
数据完整性和安全通讯

D. Security Manager and Related Functions
安全经理和相关权限

2. Authentication Methods 认证方式

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.

本安全程序包括特定的安全认证方式（"认证方式"），该等认证方式将通过诸如用户ID /密码对、数字证书、生物特征、安全令牌（通过硬件或软件部署）、印章/签字验证，和/或与认证方式关联的设备等一个或多个组合的验证方法（统称为 "密钥"）来识别和验证客户和/或其授权的任何用户的权限。 通过这些认证方式和相关密钥，银行可以验证所收到通讯的来源。

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.

您可登录CitiDirect 网银系统的登录帮助网站以了解更多与登录服务和/或连接渠道的认证方式相关的信息。客户可以随时选择一种适用的认证方式。在设置服务或连接渠道时，银行会设置一种默认的认证方式，客户可以随时更改至另一种适用的认证方式。

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

以下认证方式可用于访问上述服务和/或连接渠道:

CitiDirect Authentication Methods CitiDirect 认证方式	
Biometrics 生物特征	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. 一种数字化认证方式，其利用用户独特的物理特征（例如指纹和面部识别）、用户移动设备上内置的生物识别技术及加密技术来访问CitiDirect。当用户选择此认证方式时，物理特征数据不会传输至银行。

CitiDirect Authentication Methods CitiDirect 认证方式	
Mobile Token (non-application based) 移动令牌 （非应用型）	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. 一种基于移动端的非应用型数字认证方式（例如，非应用型移动令牌），通过加密密钥与生物特征认证（如指纹和面部识别），借助用户移动浏览器将其移动设备与CitiDirect账户绑定。当用户选用此认证方式时，其生物特征数据不会向银行传输。该方式通过对用户已注册的移动设备进行身份验证，从而实现多因素认证。
Challenge Response Token 询问应答令牌	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. （i）基于移动应用程序的软令牌（例如MobilePASS）或（ii）物理令牌（例如SafeWord卡、Vasco），用于在使用数字认证（例如4位数字认证）之后生成动态密码。 当访问CitiDirect 时，系统生成一个询问码，并且通过所使用的令牌生成应答码并输入到系统中。该认证方式搭配安全密码使用构成多因素认证。
One-Time Password Token 一次性密码令牌	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）基于移动应用程序的软令牌（例如MobilePASS）或（ii）物理令牌（例如SafeWord卡，Vasco），用于在使用数字认证（例如4位数字认证）之后生成动态密码。 将此动态密码输入系统以获得访问权限。
Secure Password 安全密码	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. 用户可以通过输入其安全密码访问系统。安全密码通常限制用户在系统中使用的功能，例如，用户仅可浏览特定的信息。该认证方式结合询问应答令牌构成多因素认证。
SMS One-Time Code 短信一次性密码	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. 通过短信发送给用户的动态密码，此后用户输入动态密码和安全密码以访问系统。
Voice One-Time Code 语音一次性密码	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. 通过自动语音呼叫发送给用户的动态密码，此后用户输入动态密码和安全密码以访问系统。

CitiDirect Authentication Methods CitiDirect 认证方式	
Digital Certificates 数字证书	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. 数字证书是一种经批准的认证机构颁发，用于认证和授权的电子身份证明。数字证书可归属于公司法人实体（"公司印鉴"）或个人（"个人证书"）。客户有责任根据当地法律正确验证所有代表客户行事的个人证书用户的身份。 银行和客户必须使用授权人员的数字证书，以确保所有通过公共或其他不安全网络连接所传输的通讯均已加密且受到保护。

CitiConnect for Files Authentication Methods CitiConnect for Files 认证方式	
Digital Certificates 数字证书	See description above. 请参考以上描述
IP Address Whitelist When Using CitiConnect 使用CitiConnet的 IP地址白名单	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. 某些银行接收的特定互联网通讯（例如通过虚拟专用网络（VPN）传输信息）可能还依赖于各方通过使用一个提前约定的互联网协议地址（IP地址）来进行信息交换。 银行只接受来自客户指定 IP地址发起的通讯，反之亦然； 银行只会向客户指定的IP地址传送通讯，反之亦然。该认证方式配合上述数字证书方法使用。

CitiConnect API Authentication Methods CitiConnect API 认证方式	
Digital Certificates 数字证书	See description above. 请参考以上描述
IP Address Whitelist When Using CitiConnect 使用CitiConnet时 的 IP地址白名单	See description above. 请参考以上描述

CitiConnect for SWIFT Authentication Methods CitiConnect for SWIFT 认证方式	
Digital Certificates 数字证书	See description above. Can be used in conjunction with SWIFT Authentication method below. 请参考以上描述。可以与下述SWIFT 认证方式配合使用。
SWIFT Authentication SWIFT认证	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. 银行和客户之间通过环球同业银行金融电信协会 (SWIFT) 网络传输的通讯 (包括但不限于: 账户信息、支付指令、以及对指令的修改或取消), 将按照SWIFT合同文档 (包括其不时进行的修订或补充) 项下的相关程序进行认证。该等文件包括但不限于一般条款和条件, FIN服务描述, 或其他由SWIFT发布的条款和条件。除满足SWIFT程序的要求外, 银行无须采取其他额外措施来确定该等通讯的发送人和真实性。 对SWIFT系统的任何错误或延误, 银行将不承担相关责任。同时, 客户需确保按照SWIFT要求和指定的格式和类型向银行发送通讯。 通过SWIFT设备发送或接收的传输和通讯应遵守有效的SWIFT规则和规定, 包括会员资格规则。 客户有责任熟悉并遵守SWIFT报文传输标准。

SWIFT Authentication Method SWIFT 认证方式	
SWIFT Authentication (Direct Connection for Financial Institutions) SWIFT认证（金融机构直连）	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. 银行和客户之间通过环球同业银行金融电信协会（SWIFT）网络传输的通讯（包括但不限于：账户信息、支付指令、以及对指令的修改或取消），将按照SWIFT合同文档（包括其不时进行的修订或补充）项下的相关程序进行认证。该等文件包括但不限于一般条款和条件，FIN服务描述，或其他由SWIFT发布的条款和条件。除满足SWIFT程序的要求外，银行无须采取其他额外措施来确定该等通讯的发送人和真实性。 对SWIFT系统的任何错误或延误，银行将不承担相关责任。同时， 客户需确保按照SWIFT要求和指定的格式和类型向银行发送通讯。 通过SWIFT设备发送或接收的传输和通讯应遵守有效的SWIFT规则和规定，包括会员资格规则。 客户有责任熟悉并遵守SWIFT报文传输标准。

Digital/Electronic Signature Authentication Methods for Electronic Document Submission 电子/数字化签名 适用于电子文档提交的认证方式	
Digital Signature 数字签名	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. 一种利用数字证书来验证签名、消息、软件或数字文档的真实性和完整性的电子签名。
Electronic Signature 电子签名	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. 电子签名是一种签署在合同或其他文件上的电子符号，其具有独特性，由有意签署的人使用。电子签名可以以文字、字母、数字、符号、点击网页按钮、上传传真或扫描实体签名、在触摸屏上签名或以电子形式同意任何条款和条件形式创建。 电子签名的创建是在使用人单独控 制下完成的，其通常会伴随或者协同一条数据信息，可以用于识别同意数字信息的人并认证其同意。 此类电子签名将通过银行的电子渠道依据以上的认证方式提交至银行。

Manual Initiated Funds Transfer (MIFT) Authentication Method 人工资金转账认证方式	
MIFT Authentication 人工资金转账的认证方式	Manually Initiated Funds Transfer (MIFT), including amendments, recalls, or cancelations of previous manual instructions, may be made by fax or letter or upload to CitiDirect. Not all forms are supported in all countries. Initiators are persons designated by the Customer who are authorized to initiate transactions in accordance with restrictions, if any, are identified by the Customer. Confirmers are person designated by the Customer that Bank may call back, at its discretion, for confirmation of manually initiated instructions for funds transfers. In certain countries, mobile telephone numbers are not accepted as call back numbers. Further details are provided in the applicable Country Cash Management User Guide, Global Manual Transaction Authorization or Universal Nomination Form. MIFT is to be used by the Customer as a contingency method to communicating instructions to the Bank. 人工资金转账，包括修改、召回或取消之前的人工指令，可以通过传真、信件或上传到CitiDirect网银系统来发送。每个国家所支持的形式有所区分。发起者为客户指定的人员，他们有权根据客户制定的限制（如有）发起交易。确认人是客户指定的人员，银行可自行决定以电话回拨方式确认发起资金转账的人工指令。 在某些特定国家中，不接受移动电话号码作为回拨号码。详情请参考适用国家的现金管理使用手册、全球人工交易授权或Universal Nomination Form。 人工资金转账是客户向银行发起指令的应急方法。

Mail, Fax, Email and Messenger Authentication Methods 邮件，传真，电子邮件和信使 认证方式	
Seal Image Verification 印鉴验证	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. 银行通过传真、邮件、电子邮件或信使收到的通讯（人工资金转账的要求除外），将根据客户提供至银行的授权文件或其他类似文件中所包含的印鉴进行谨慎地验证及整理。
Signature Verification 签字验证	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. 银行通过传真、邮件、电子邮件或信使收到的通讯（人工资金转账的要求除外），将根据客户提供至银行的授权文件或其他类似文件中所包含的信息进行签名验证。
Secure PDF 安全PDF	Encrypted emails are delivered to a regular mailbox as PDF documents that are opened by entering a private password. Both the message body and any attached files are encrypted. A private password can be set up upon receipt of the first secure email received. 加密的电子邮件将作为PDF文档传送至常规邮箱，通过输入专属密码打开。邮件正文及其任何附件均已加密。在收到第一封安全电子邮件后，可以设置专属密码。
MTLS 强制性传输层协议	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. 强制性传输层协议（MTLS）在银行和客户之间创建了一个安全的专属电子邮件连接。使用此渠道发送的电子邮件由一个通过连接创建的加密TLS通道通过互联网发送。

Phone Authentication Methods 电话 认证方式	
PIN 密码	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. 客户通过电话联系银行时，将提示您通过输入一串密码验证访问权限。
Verification Questions 验证问题	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. 当客户通过电话联系银行时，银行服务代表将提示您对验证问题提供正确的口头答复以验证访问权限。

The availability of Authentication Methods described above varies based on local markets.
以上描述的认证方式的可用性因当地市场而异。

3. Customer Responsibilities
客户职责

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.

识别授权用户：客户负责识别：(i) 对于所有服务和连接渠道在公司层面代表客户对账户行事的所有个人；和 (ii) 每一个被客户正式授权并代表客户对客户账户行事的人。

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.

客户负责分配和监控分配给客户和/或其用户的交易限额，并确保这些限额 (a) 不超过客户公司内部政策、其他授权和组织性文件 (例如客户的董事会决议、银行委托书、授权委托书，或同等文件) 规定的上限；(b) 将正确反应在所有连接渠道和用户权限上。

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.

某些司法管辖区可能要求银行在向个人授予访问权限以操作某些功能之前，先确认其 (及其相应的密钥) 符合适用的反洗钱法律要求。如需更多信息，请联系您的客户服务代表或者访问CitiDirect 网站。

3.4 Safeguarding of Authentication Methods
认证方式的保护

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.

客户有责任以最高标准的谨慎程度保护其认证方式和密钥，并确保对密钥的访问和分发仅限于客户的授权人。

第三方发送的通讯：当客户使用密钥识别和认证其作为法人实体发出的通讯时，客户有责任在向银行发送通讯时对密钥的使用行使完全的掌控权，包括当该等通讯是由代表客户管理应用和/或系统的第三方发送的。在任何情况下，银行会 (a) 将自电子连接渠道接收的、已由银行根据安全程序经正式认证为来自于客户的通讯视为客户所指示的通讯；以及 (b) 依照安全程序代表客户对于收到的通讯进行操作。

4. Data Integrity and Secured Communications
数据完整性和安全通讯

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.

客户在通过使用互联网、邮件、电子邮件和/或传真的方式向银行传输数据或与银行交换通讯时，客户了解该等方式 (1) 均不一定为安全的通讯和传输系统；(2) 均不在银行的控制范围内。客户进一步知悉，若其用户有权访问开放银行及/或花旗系统外部的类似第三方平台，则客户数据可能通过该等不受银行控制的第三方平台进行传输。

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.

银行采用行业领先的加密方式 (具体方式由银行确定)，其有助于确保信息保密，同时保证信息在电子传输过程中不被篡改。

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.

如果客户怀疑或意识到技术故障，或怀疑、意识到任何人 (无论是否为授权人员) 对银行服务、连接渠道或认证方式存在不当或潜在欺诈性的访问或使用时，客户应及时通知银行。 如果授权人存在不当或潜在欺诈的访问或使用，客户应立即采取行动，终止该授权人员访问和使用银行服务或连接渠道。

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.

如果客户使用文件格式化或加密软件 (无论由银行或第三方提供) 以支持客户数据和指令的格式化与识别，以及与银行通讯时所采取的行动，则客户应仅为其安装该软件的目的使用该软件。

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.

以下两种情况下，客户接受银行可能会中止或拒绝用户需要使用密钥访问的服务：(1) 怀疑未经授权或欺诈性地使用密钥，和/或 (2) 为保障服务或密钥的安全。

5. Security Manager and Related Functions
安全经理和相关权限

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:

对于CitiDirect网银系统和CitiConnect可访问的应用程序(除以下所述个人证书的情况外), 银行要求客户设立 "安全经理" 职能。安全经理对以下操作负责:

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);

建立和维护用户 (包括安全经理本身) 的访问和权限, 包括以下活动: (a) 创建、删除或修改用户配置文件 (包括安全经理配置文件) 和权限 (请注意, 用户名必须与证明身份的证件一致) (b) 建立访问配置文件, 定义个人用户可使用的功能和数据 (c) 启用和禁用用户登录密钥 (d) 分配交易限额 (请注意, 对于限额的设置, 银行不会予以监控和核实。客户需要自行监测该等限额, 以保证其符合客户的内部政策和要求, 包括但不限于客户董事会或同等机构制定的内部政策和要求);

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;

在客户维护的库中创建和修改条目 (例如预格式化付款和受益人库), 并授权其他用户执行相同操作;

5.3 Modifying payment authorization flows;

修改付款授权流程;

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

将动态密码密钥或其他系统访问密钥或密码分发给客户的用户;

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

如果有任何理由怀疑账户安全受到损害, 通知银行; 以及

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

管理和获取数字证书并授权其他用户执行相同操作。

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.

请注意: 安全经理的角色和责任可能会因为某些当地市场的监管要求和/或运营能力而有所不同或不可适用。 在该等市场中, 银行可要求客户提供额外的文件和其他信息以代客户履行安全经理的权限。

6. Use of CitiDirect and CitiConnect by Security Managers 安全经理对CitiDirect 网银系统和CitiConnect的使用

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.

银行需要两名不同的人员来输入和授权指令; 因此, 至少需要两 (2) 名安全经理。任何两名安全经理协同行动, 可 以通过与任何安全经理的职能相关或协助通讯相关的连接渠道发送指令和/或提供确认。任何该等两名安全经理 授权的通讯, 银行均接受并据此行事, 该等通讯视为由客户提供。银行建议至少指定三名安全经理以确保充足的后备人员。客户应在财资贸易方案电子渠道登记表上指定其安全经理。客户的安全经理无需进一步指定, 也可以担任第三方实体 (例如客户的关联机构) 的安全经理, 并行使与之相关的所有权利 (包括对第三方实体的账户用户的任命), 前提是该第三方实体签署了授予客户访问其账户权限的全球访问授权书 (或银行接受的其他形式的授权书)。其仅适用于相关授权下涵盖的账户。

7. Use of CitiDirect by Security Officers (For Personal Certificates only) 安全主管对CitiDirect 网银系统的使用 (仅限个人证书)

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.

银行需要两名不同的人员来管理发放给个人的数字证书 ("个人证书")。因此, 需要两 (2) 名安全主管向用户分发和收回个人证书, 以便认证和授权连接渠道的通讯。银行建议指定至少三名安全主管以确保有充足的后备人员。任何来自个人证书授权的通讯, 银行均接受并据此行事, 该等通讯视为由客户提供。

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions