Security Procedures
Quy trình Bảo mật

1. Introduction
Giới thiệu

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).

Những "Quy trình Bảo mật" này, đã được đề cập trong mục Trao đổi thông tin trong Điều khoản chung về Tài khoản và Dịch vụ ("MAST") (hoặc các điều khoản và điều kiện tài khoản khác), được thiết kế nhằm mục đích xác thực việc truy cập của Khách hàng tới các kênh kết nối của Ngân hàng và xác minh nguồn gốc của việc Trao đổi thông tin giữa Ngân hàng và Khách hàng liên quan tới các Dịch vụ hoặc kênh kết nối sau đây (tùy vào dịch vụ được cung cấp tại các thị trường địa phương).

- CitiDirect BE® (including WorldLink®)
  CitiDirect BE® (bao gồm WorldLink®)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  Lệnh Giao dịch bằng hình thức thủ công
- Interactive Voice Response ("IVR")
  Tương tác trả lời tự động (IVR)
- Email/Fax/Mail/Messenger/Phone with the Bank
  Thư Điện tử/Fax/Thư/Tin nhắn/Điện thoại với Ngân hàng
- Other local electronic connectivity channels
  Các kênh kết nối điện tử tại địa phương khác

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:

Những Quy trình Bảo mật này được đọc cùng với MAST và có thể được cập nhật và hướng dẫn tới Khách hàng tùy từng thời điểm bằng các hình thức điện tử hoặc các hình thức khác, bao gồm nhưng không giới hạn cho việc đăng tải cập nhật Quy trình Bảo mật trên CitiDirect BE. Trừ trường hợp được luật pháp quy định khác, việc tiếp tục sử dụng các dịch vụ hoặc kênh kết nối trên của Khách hàng sau khi được hướng dẫn về cập nhật Quy trình Bảo mật sẽ bao gồm sự chấp thuận của Khách hàng về những cập nhật Quy trình Bảo mật này. Những Quy trình Bảo mật bao gồm:

A. Authentication Methods
Phương thức Xác thực

B. Customer Responsibilities
Trách nhiệm Khách hàng

C. Data Integrity and Secured Communications
Thông tin trung thực và Trao đổi thông tin Bảo mật

D. Security Manager and Related Functions
Người Quản lý Bảo mật và các Chứng năng liên quan

2. Authentication Methods
Phương thức Xác thực

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.

Những Quy trình Bảo mật này bao gồm các phương thức xác thực an toàn ("Phương thức xác thực") được sử dụng để xác định cụ thể và xác minh ủy quyền của Khách hàng và/hoặc bất kỳ người dùng nào được ủy quyền bởi Khách hàng, điển hình qua một hoặc kết hợp nhiều cơ chế như kết hợp cặp ID/mật khẩu người dùng, chứng thư số, sinh trắc học, mã an ninh token (được sử dụng qua thiết bị vật lý hoặc phần mềm), xác thực đóng dấu/chữ ký, và/hoặc thiết bị liên quan tới các Phương thức xác thực (gọi chung là "Chứng chỉ chứng thực"). Phương thức Xác thực và các Chứng chỉ chứng thực liên quan cho phép Ngân hàng xác minh nguồn gốc của Trao đổi thông tin Ngân hàng nhận được.

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.

Các thông tin về Phương thức Xác thực đối với truy cập Dịch vụ và/hoặc các kênh kết nối có thể được tham khảo tại trang website Trợ giúp Truy cập CitiDirect BE. Khách hàng có thể lựa chọn Phương thức Xác thực sẵn có bất kỳ thời điểm nào. Trong khi thiết lập cài đặt Dịch vụ hoặc các kênh kết nối, Ngân hàng có thể cài đặt mặc định Phương thức Xác thực mà Khách hàng có thể thay đổi tại bất kỳ thời điểm nào.

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

Các Phương thức Xác thực sau đây sẵn có để truy cập dịch vụ và/hoặc các kênh kết nối:

CitiDirect BE Authentication Methods *CitiDirect BE Phương thức xác thực*	
Biometrics *Sinh trắc học*	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. *Phương thức xác thực sử dụng đặc điểm vật lý cá biệt của người dùng (ví dụ như vân tay hoặc nhận dạng khuôn mặt), công nghệ sinh trắc học thiết lập bên trong thiết bị di động của người dùng, và công nghệ mật mã học để truy cập vào CitiDirect BE. Dữ liệu đặc điểm vật lý không được chuyển cho Ngân hàng khi người dùng lựa chọn phương thức xác thực này.*
Challenge Response Token *Mã Phản hồi Thách thức*	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. *Với (i) ứng dụng điện thoại sử dụng mã mật khẩu mềm (MobilePASS) hoặc (ii) mã vật lý (Safeword Card, Vasco), trong từng trường hợp tạo mật khẩu động sau khi xác thực với mã PIN (ví dụ PIN 4 chữ số). Khi truy cập CitiDirect BE, hệ thống gửi ra mã thách thức và mã phản hồi được tạo với token được sử dụng và nhập vào hệ thống. Phương thức xác thực này khi được kết hợp với mật khẩu bảo mật sẽ tạo ra xác thực đa lớp.*
One-Time Password Token *Mã Mật khẩu Một lần*	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. *Hoặc (i) ứng dụng điện thoại sử dụng mã mật khẩu mềm (MobilePASS) hoặc (ii) mã vật lý (Safeword Card, Vasco) được sử dụng để tạo mật khẩu động sau khi xác thực với mã PIN (ví dụ PIN 4 chữ số). Mật khẩu động được nhập vào hệ thống để truy cập.*
Secure Password *Mật khẩu Bảo mật*	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. *Người dùng sử dụng Mật khẩu Bảo mật của mình để truy cập hệ thống. Mật khẩu Bảo mật hạn chế khả năng truy cập của người dùng vào hệ thống, ví dụ, chỉ cho phép một số thông tin cụ thể được người dùng xem. Phương thức xác thực này khi được kết hợp với Mã Phản hồi Thách thức sẽ tạo ra xác thực đa lớp.*
SMS One-Time Code *Mã SMS Một lần*	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. *Mật khẩu động được gửi cho người dùng qua SMS, sau đó người dùng sẽ nhập mật khẩu động này và Mật khẩu Bảo mật để truy cập hệ thống.*
Voice One-Time Code *Mã Giọng nói Một lần*	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. *Mật khẩu động được gửi cho người dùng qua Tương tác trả lời tự động, sau đó người dùng sẽ nhập mật khẩu động này và Mật khẩu Bảo mật để truy cập hệ thống.*

Digital Certificates *Chứng thư số*	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. *Chứng thư số là một định dạng điện tử được cấp bởi cơ quan có thẩm quyền phê duyệt chứng thư số để xác thực và ủy quyền. Chứng thư số có thể sử dụng cho doanh nghiệp ("Con dấu công ty") và cá nhân ("Chứng thư cá nhân"). Khách hàng chịu trách nhiệm xác thực các định danh người dùng Chứng thư cá nhân hoạt động trên danh nghĩa của Khách hàng theo luật địa phương.* 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. *Ngân hàng và Khách hàng được yêu cầu sử dụng Chứng thư số do người được ủy quyền cung cấp, nhằm đảm bảo các Trao đổi thông tin qua kết nối Internet công cộng hoặc kết nối không bảo mật được mã khóa và bảo vệ hoàn toàn.*

CitiConnect for Files Authentication Methods *CitiConnect đối với Files Phương thức xác thực*	
Digital Certificates *Chứng thư số*	See description above. *Xem mô tả bên trên*
IP Address Whitelist When Using CitiConnect *Địa chỉ IP Danh sách trắng Khi sử dụng 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. *Trao đổi thông tin Internet được nhận bởi Ngân hàng, ví dụ, qua Mạng riêng ảo (VPN), cũng có thể phụ thuộc vào bên trao đổi thông tin sử dụng địa chỉ Internet Protocol thỏa thuận trước. Ngân hàng sẽ chỉ chấp nhận trao đổi thông tin từ địa chỉ IP được chỉ định của Khách hàng, và ngược lại, Ngân hàng sẽ chỉ truyền Thông tin trao đổi tới địa chỉ IP được đăng ký của Khách hàng, và ngược lại. Được sử dụng cùng với phương thức Chứng thư số ở trên.*

CitiConnect API Authentication Methods *CitiConnect API Phương thức xác thực*	
Digital Certificates *Chứng thư số*	See description above. *Xem mô tả bên trên*
IP Address Whitelist When Using CitiConnect *Địa chỉ IP Danh sách trắng Khi sử dụng CitiConnect*	See description above. *Xem mô tả bên trên*

CitiConnect for SWIFT Authentication Methods *CitiConnect đối với SWIFT Phương thức xác thực*	
Digital Certificates *Chứng thư số*	See description above. Can be used in conjunction with SWIFT Authentication method below. *Xem mô tả bên trên. Có thể sử dụng cùng với Phương thức Xác thực SWIFT ở trên.*
SWIFT Authentication *Xác thực 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. *Trao đổi thông tin giữa Ngân hàng và Khách hàng qua SWIFT, bao gồm nhưng không giới hạn thông tin tài khoản, yêu cầu thanh toán, và các yêu cầu thay đổi hoặc hủy các lệnh đó, sẽ được xác thực sử dụng quy trình được nêu trong Chứng từ Hợp đồng SWIFT (được thay đổi hoặc bổ sung tại các thời điểm) bao gồm không giới hạn các Điều khoản và Điều kiện và Mô tả Dịch vụ FIN hoặc được nêu trong các Điều khoản và Điều kiện khác được SWIFT thiết lập. Ngân hàng không có nghĩa vụ phải thực hiện bất kỳ điều gì ngoài những điều được nêu trong quy trình SWIFT để đăng ký người gửi và xác thực các phương thức trao đổi thông tin này.* 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. *Ngân hàng không chịu trách nhiệm cho bất kỳ lỗi hoặc chậm nghẹ trễ nào trên hệ thống SWIFT. Khách hàng chịu trách nhiệm cung cấp trao đổi thông tin tới Ngân hàng theo định dạng và loại hình yêu cầu cụ thể bởi 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. *Việc truyền dữ liệu và Thông tin trao đổi được gửi và nhận qua SWIFT sẽ phải tuân thủ quy tắc và quy định SWIFT hiện hành. Khách hàng chịu trách nhiệm làm quen và tuân thủ tiêu chuẩn tin nhắn SWIFT.*

SWIFT Authentication Method *SWIFT Phương thức xác thực*	
SWIFT Authentication (Direct Connection for Financial Institutions) *Xác thực SWIFT (Kết nối trực tiếp đối với các Tổ chức Tài chính)*	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. *Trao đổi thông tin giữa Ngân hàng và Khách hàng qua SWIFT, bao gồm nhưng không giới hạn thông tin tài khoản, yêu cầu thanh toán, và các yêu cầu thay đổi hoặc hủy các lệnh đó, sẽ được xác thực sử dụng quy trình được nêu trong Chứng từ Hợp đồng SWIFT (được thay đổi hoặc bổ sung tại các thời điểm) bao gồm không giới hạn các Điều khoản và Điều kiện và Mô tả Dịch vụ FIN hoặc được nêu trong các Điều khoản và Điều kiện khác được SWIFT thiết lập. Ngân hàng không có nghĩa vụ phải thực hiện bất kỳ điều gì ngoài những điều được nêu trong quy trình SWIFT để đăng ký người gửi và xác thực các phương thức trao đổi thông tin này.* 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. *Ngân hàng không chịu trách nhiệm cho bất kỳ lỗi hoặc chậm nghệ trễ nào trên hệ thống SWIFT. Khách hàng chịu trách nhiệm cung cấp trao đổi thông tin tới Ngân hàng theo định dạng và loại hình yêu cầu cụ thể bởi 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. *Việc truyền dữ liệu và Thông tin trao đổi được gửi và nhận qua SWIFT sẽ phải tuân thủ quy tắc và quy định SWIFT hiện hành. Khách hàng chịu trách nhiệm làm quen và tuân thủ tiêu chuẩn tin nhắn SWIFT.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission *Chữ ký Số/Chữ ký Điện tử Phương thức xác thực*	
Digital Signature *Chữ ký Số*	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. *Một loại chữ ký điện tử sử dụng chứng thư số để xác nhận tính xác thực và chân thực của chữ ký, tin nhắn, phần mềm hoặc văn bản điện tử.*

Electronic Signature *Chữ ký Điện tử*	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. *Một ký hiệu điện tử đính kèm với hợp đồng hoặc bản ghi khác, cá biệt và được sử dụng bởi một người với mục đích ký. Chữ ký điện tử có thể được thiết lập dưới dạng chữ, từ, số, ký hiệu, nhấp chuột vào một ô trên website, đăng tải fax hoặc scan của chữ ký vật lý, ký trên màn hình cảm ứng, hoặc đồng ý với bất kỳ điều khoản và điều kiện nào với hình thức điện tử. Được tạo ra dưới sử kiểm soát duy nhất của người sử dụng, chúng được đính kèm một cách logic hoặc liên kết với dữ liệu tin nhắn, có thể xác định người đồng ý với dữ liệu tin nhắn đó và xác nhận sự đồng ý của người đó. Chữ ký điện tử có thể được nộp cho Ngân hàng qua các kênh điện tử của Ngân hàng và tuân thủ Phương thức Xác thực liên quan được mô tả ở trên.*

Manual Initiated Funds Transfer (MIFT) Authentication Method ***Giao dịch sử dụng phương thức thủ công (MIFT) Phương thức xác thực***	
MIFT Authentication *Xác thực MIFT*	Manually Initiated Funds Transfer (MIFT), including amendments, recalls, or cancelations of previous manual instructions, may be made by fax or letter or upload to CitiDirect. Not all forms are supported in all countries. Initiators are persons designated by the Customer who are authorized to initiate transactions in accordance with restrictions, if any, are identified by the Customer. Confirmers are person designated by the Customer that Bank may call back, at its discretion, for confirmation of manually initiated instructions for funds transfers. *Lệnh Giao dịch sử dụng phương thức thủ công (MIFT), bao gồm các yêu cầu thay đổi, truy hồi hoặc hủy các lệnh thủ công trước đó, có thể được thực hiện bằng fax hoặc thư hoặc đăng tải trên CitiDirect. Không phải tất cả các cách đều được các quốc gia hỗ trợ. Người khởi tạo lệnh là người được chỉ định bởi Khách hàng ủy quyền thực hiện giao dịch với các hạn chế, nếu có, được xác định bởi Khách hàng. Người xác thực lệnh là người được chỉ định bởi Khách hàng, trong đó Ngân hàng có thể gọi điện xác thực, theo quyết định của Ngân hàng, để yêu cầu xác thực các lệnh được khởi tạo thủ công đối với các lệnh chuyển tiền.* 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. *Tại một số quốc gia, số điện thoại di động không được chấp nhận cho mục đích gọi xác nhận. Chi tiết được cung cấp trong Hướng dẫn sử dụng dịch vụ tiền tệ tại các quốc gia áp dụng, Ủy quyền giao dịch Toàn cầu hoặc Mẫu đơn Chỉ định Toàn cầu. MIFT được Khách hàng sử dụng như hình thức dự phòng để liên hệ với Ngân hàng.*

Mail, Fax, Email and Messenger Authentication Methods *Thư, Fax, Email và Tin nhắn Phương thức xác thực*	
Seal Image Verification *Xác thực Hình ảnh đóng dấu*	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. *Thông tin nhận được bởi Ngân hàng qua fax, thư, email hoặc tin nhắn, không bao gồm các yêu cầu lệnh MIFT, được xác thực và đối chiếu kỹ càng dựa trên hình ảnh đóng dấu trên chứng từ thẩm quyền của Khách hàng hoặc các chứng từ tương tự được cung cấp cho Ngân hàng.*
Signature Verification *Xác thực chữ ký*	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. *Thông tin nhận được bởi Ngân hàng qua fax, thư, email hoặc chữ ký, không bao gồm các yêu cầu lệnh MIFT, được xác thực chữ ký dựa trên thông tin trên chứng từ thẩm quyền của Khách hàng hoặc các chứng từ tương tự được cung cấp cho Ngân hàng.*
Secure PDF *PDF Bảo mật*	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. *Các email được mã hóa chuyển tới hòm thư thông thường là các chứng từ định dạng PDF được mở với mật khẩu riêng biệt. Cả thông tin nội dung và bất kỳ tập file đính kèm nào cũng được mã hóa. Một mật khẩu riêng biệt có thể được cài đặt khi nhận được thư bảo mật đầu tiên.*
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. *An ninh theo lớp vận chuyển bắt buộc (MLTS) tạo ra liên kết email bảo mật, cá biệt giữa Ngân hàng và Khách hàng. Email được truyền qua kênh này được chuyển qua Internet qua đường dẫn TLS được mã hóa tạo ra bởi liên kết này.*

Phone Authentication Methods *Điện thoại Phương thức xác thực*	
PIN *PIN*	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *Khách hàng liên hệ với Ngân hàng qua điện thoại được yêu cầu nhập mã PIN để xác thực truy cập được ủy quyền.*
Verification Questions *Câu hỏi Xác thực*	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. *Khách hàng liên hệ với Ngân hàng qua điện thoại được yêu cầu bởi đại diện dịch vụ Ngân hàng đưa ra câu trả lời đúng bằng lời nói đối với các câu hỏi xác thực để có thể xác thực truy cập được ủy quyền.*

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

Sự sẵn có của Các Phương thức Xác thực nêu trên thay đổi tại các thị trường địa phương.

3. Customer Responsibilities
Trách nhiệm Khách hàng

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.

Xác định Người dùng được ủy quyền: Khách hàng có trách nhiệm xác định: (i) tất cả các cá nhân được hoạt động Tài khoản thay mặt cho Khách hàng tại cấp tổ chức đối với tất cả các Dịch vụ và các kênh kết nối, và (ii) mỗi người hoạt động thay mặt cho Khách hàng được ủy quyền đầy đủ bởi Khách hàng đối với việc hoạt động trên tài khoản Khách hàng.

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.

Khách hàng chịu trách nhiệm chỉ định và quản lý hạn mức giao dịch được chỉ định cho Khách hàng và/hoặc người dùng của Khách hàng và đảm bảo rằng những hạn mức đó (a) không vượt quá hạn mức được yêu cầu trong chính sách nội bộ và các chứng từ ủy quyền và thành lập của Khách hàng ví dụ như Nghị quyết Hội đồng Quản trị của Khách hàng, Ủy quyền Ngân hàng, Thư Ủy Quyền, hoặc các chứng từ tương tự, và (b) được thể hiện đầy đủ tại các tất cả các kênh kết nối và quyền người dùng.

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.

Một số quốc gia có thể yêu cầu các cá nhân (và các Chứng chỉ chứng thực tương ứng của họ) được xác định bởi Ngân hàng theo yêu cầu luật phòng chống rửa tiền AML trước khi trao quyền thực hiện một số chức năng nhất định. Vui lòng liên hệ Người đại diện Dịch vụ Khách hàng của Quý khách hoặc truy cập website CitiDirect BE để biết thêm thông tin.

3.4 Safeguarding of Authentication Methods

Bảo vệ các Phương thức Bảo mật

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.

Khách hàng chịu trách nhiệm bảo vệ các Phương thức Bảo mật và Chứng chỉ chứng thực với tiêu chuẩn cẩn thận và cẩn trọng cao nhất, và đảm bảo rằng việc truy cập và thông báo Chứng chỉ chứng thực chỉ được giới hạn cho những người được Khách hàng ủy quyền truy cập.

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.

Trao đổi thông tin được gửi bởi bên thứ ba: Khi Khách hàng sử dụng Chứng chỉ chứng thực để xác định và xác minh việc Trao đổi thông tin của họ được xuất phát từ họ như một pháp nhân, Khách hàng chịu trách nhiệm thực hiện kiểm soát hoàn toàn đối với những Chứng chỉ chứng thực đó khi gửi những Thông tin trao đổi tới Ngân hàng, bao gồm khi các Thông tin trao đổi này được gửi bằng các ứng dụng và/ hoặc hệ thống được quản lý bởi bên thứ ba thay mặt cho Khách hàng. Trong tất cả các trường hợp, Ngân hàng sẽ (a) coi Thông tin trao đổi nhận được qua kênh kết nối điện tử, đã được nhận bởi Ngân hàng theo Quy trình Bảo mật được xác thực đầy đủ là xuất phát từ Khách hàng, là Trao đổi thông tin được yêu cầu bởi Khách hàng và (b) có thể thực hiện trên các Thông tin Trao đổi này khi nhận được thay mặt cho Khách hàng theo Quy trình Bảo mật này.

4. Data Integrity and Secured Communications
Thông tin Trung thực và Trao đổi thông tin An toàn

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.

Khách hàng sẽ truyền dữ liệu, hoặc trao đổi Thông tin với Ngân hàng, sử dụng Internet, Thư, Thư điện tử và/hoặc fax mà Khách hàng hiểu rằng (i) không nhất thiết là phương thức trao đổi thông tin và hệ thống truyền tải an toàn, và (ii) không dưới sự kiểm soát của Ngân hàng.

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.

Ngân hàng, sử dụng các phương thức mã hóa dẫn đầu thị trường (được quyết định bởi Ngân hàng), trong đó giúp đảm bảo thông tin được bảo mật và không thay đổi khi truyền tải điện tử.

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.

Nếu Khách hàng nghi ngờ hoặc biết về các lỗi kỹ thuật, hay bất kỳ sự truy cập hoặc sử dụng trái phép hoặc có khả năng gian lận đối với Dịch vụ Ngân hàng hoặc các kênh kết nối hoặc Phương thức xác thực bởi bất kỳ ai (dù được ủy quyền hay không), Khách hàng phải thông báo kịp thời cho Ngân hàng về các trường hợp trên. Trong trường hợp xảy ra việc truy cập hoặc sử dụng trái phép hoặc có khả năng gian lận bởi một người được ủy quyền, Khách hàng cần ngay lập tức ngừng cho phép quyền truy cập và sử dụng Dịch vụ hoặc các kênh kết nối của người được ủy quyền này.

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.

Nếu Khách hàng sử dụng phần mềm định dạng tập thông tin hoặc mã hóa (được Ngân hàng hay bên thứ ba cung cấp) để hỗ trợ việc định dạng và nhận dạng dữ liệu và chỉ thị yêu cầu của Khách hàng và thực hiện Trao đổi Thông tin với Ngân hàng, Khách hàng phải sử dụng những phần mềm này riêng biệt cho mục đích mà phần mềm được cài đặt.

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.

Khách hàng chấp nhận rằng Ngân hàng có thể dừng hoặc từ chối quyền truy cập người dùng sử dụng các Dịch vụ yêu cầu Chứng chỉ Chứng thực (i) trong trường hợp nghi ngờ việc sử dụng không được ủy quyền hoặc gian lận những Chứng chỉ chứng thực đó và/hoặc (ii) bảo vệ Dịch vụ hoặc các Chứng chỉ chứng thực.

5. Security Manager and Related Functions
Quản lý An ninh và các chứng năng liên quan

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:

Đối với các ứng dụng có thể truy cập trên CitiDirect BE (trừ các trường hợp Chứng thư Cá nhân được đề cập dưới đây), Ngân hàng yêu cầu Khách hàng thiết lập chức năng "Quản lý Bảo mật". Người Quản lý Bảo mật có trách nhiệm:

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);

Thiết lập và duy trì truy cập và quyền người dùng (bao gồm cả Quản lý Bảo mật) gồm có các hoạt động ví dụ như sau: (a) tạo, xóa hoặc thay đổi hồ sơ người dùng (bao gồm cả hồ sơ Quản lý Bảo mật) và phân quyền (Lưu ý rằng tên người dùng phải đúng với các chứng từ định danh); (b) xây dựng hồ sơ truy cập trong đó xác định chức năng và dữ liệu sẵn có với từng cá nhân người dùng; (c) cho phép và không cho phép chứng chỉ truy cập người dùng; và (d) chỉ định hạn mức giao dịch (Lưu ý những hạn mức này không được quản lý hoặc xác thực bởi Ngân hàng và Khách hàng phải quản lý những hạn mức này để đảm bảo chúng tuân thủ với các chính sách nội bộ và yêu cầu của Khách hàng, bao gồm nhưng không giới hạn, cho những hạn mức được lập ra bởi Hội đồng Quản trị của Khách hàng hoặc tương tự);

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;

Tạo và thay đổi thông tin trong thư viện lưu trữ Khách hàng (ví dụ như thông tin người thụ hưởng và thanh toán được định dạng trước) và ủy quyền những người dùng khác thực hiện tương tự;

5.3 Modifying payment authorization flows;

Thay đổi quy trình duyệt thanh toán;

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

Phân bổ thông tin xác thực mật khẩu động hoặc thông tin truy cập hệ thống khác hoặc mật khẩu cho Người dùng của Khách hàng; và

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

Thông báo cho Ngân hàng nếu có bất kỳ lý do nào để nghi ngờ rằng an ninh đang bị xâm phạm.

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.

Lưu ý: Vai trò và Trách nhiệm của Người Quản lý Bảo mật có thể thay đổi hoặc không áp dụng tại một số thị trường nhất định do quy định luật pháp và/hoặc khả năng vận hành. Tại các thị trường này, Ngân hàng có thể yêu cầu các chứng từ bổ sung và các thông tin khác từ Khách hàng để thực hiện chức năng của Người Quản lý Bảo mật thay mặt cho Khách hàng.

6. Use of CitiDirect BE by Security Managers
Sử dụng CitiDirect BE của Người Quản lý Bảo mật

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.

Ngân hàng yêu cầu hai (2) cá nhân riêng biệt được nhập thông tin và ủy quyền các giao dịch; do vậy, tối thiểu hai Người Quản lý Bảo mật được yêu cầu. Bất kỳ hai Người Quản lý Bảo mật nào, cùng hành động, được đưa ra chỉ thị và/hoặc xác thực qua các kênh kết nối liên quan tới vai trò của Người Quản lý Bảo mật hoặc về liên quan tới việc hỗ trợ trao đổi thông tin. Bất kỳ trao đổi thông tin nào, khi được ủy quyền bởi hai Người Quản lý Bảo mật, sẽ được chấp nhận và thực hiện bởi Ngân hàng và được coi là được Khách hàng đưa ra. Ngân hàng khuyến nghị việc chỉ định tối thiểu ba Người Quản lý Bảo mật để đảm bảo hỗ trợ kịp thời khi cần thiết. Khách hàng cần chỉ định Người Quản lý Bảo mật của Khách hàng trên Mẫu đơn TTS Channels Onboarding Form. Một Người Quản lý thông tin của Khách hàng cũng có thể thực hiện như là Người Quản lý thông tin cho bên thứ ba (ví dụ, bên liên kết của Khách hàng) và thực hiện tất cả các quyền liên quan theo sau (bao gồm chỉ định người dùng cho tài khoản của bên thứ ba), mà không cần tới các chỉ định khác, nếu bên thứ ba thực hiện Mẫu đơn Universal Access Authority Form (hoặc nếu mẫu đơn khác về việc ủy quyền được Ngân hàng chấp nhận) cho phép Khách hàng truy cập các tài khoản của họ. Điều này chỉ áp dụng đối với các Tài khoản được nêu trong các ủy quyền liên quan.

7. Use of CitiDirect BE by Security Officers (For Personal Certificates only)
Sử dụng CitiDirect BE bởi Cán bộ Bảo mật (Chỉ áp dụng đối với Chứng thư cá nhân)

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.

Ngân hàng yêu cầu (2) hai cá nhân riêng biệt quản lý chứng thư số thuộc về cá nhân ("Chứng thư cá nhân"). Do vậy, hai Cán bộ Bảo mật được yêu cầu chỉ định và loại bỏ Chứng thư Cá nhân cho người dùng, với mục đích xác thực và ủy quyền Trao đổi thông tin trên các kênh kết nối. Ngân hàng khuyến nghị việc chỉ định ít nhất ba Cán bộ Bảo mật để đảm bảo hỗ trợ đầy đủ khi cần thiết. Bất kỳ Trao đổi thông tin được ủy quyền bởi Chứng thư cá nhân sẽ được chấp nhận và thực hiện bởi Ngân hàng và được xem như đã được yêu cầu bởi Khách hàng.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions