Treasury and Trade Solutions

Security Procedures

الإجراءات الأمنية

1. Introduction

1. مقدمة

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).

تم تصميم "إجراءات الأمان" الماثلة، كما هو مشار إليه في قسم الاتصالات في الحساب الرئيسي وشروط الخدمة ("MAST") (أو شروط وأحكام الحساب الأخرى المنطبقة)، للمصادقة على تسجيل دخول العميل إلى قنوات اتصال البنك والتحقق من مصادر الاتصالات بين البنك والعميل فيما يتعلق بالخدمات أو قنوات الاتصال التالية (قد يختلف مدى توفرها عبر الأسواق المحلية).

- CitiDirect® (including WorldLink®)

  CitiDirect® بما في ذلك (WorldLink®)

- CitiConnect®

  CitiConnect®

- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")

  جمعية الاتصالات المالية العالمية بين البنوك (سويفت "SWIFT")

- Manual Initiated Funds Transfer ("MIFT")

  التحويل اليدوي للأموال ("MIFT")

- Interactive Voice Response ("IVR")

  الاستجابة الصوتية التفاعلية ("IVR")

- Email/Fax/Mail/Messenger/Phone with the Bank

  البريد الإلكتروني/ الفاكس/ البريد/ المراسلة/ الهاتف مع البنك

- Other local electronic connectivity channels

  قنوات الاتصال الإلكترونية المحلية الأخرى

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:

يجب قراءة إجراءات الأمان هذه مع الحساب الرئيسي وشروط الخدمة MAST ويمكن تحديثها وإبلاغ العميل بها من وقت لآخر من خلال وسائل إلكترونية أو غيرها، بما في ذلك على سبيل المثال لا الحصر نشر التحديثات على إجراءات الأمان على CitiDirect®. ما لم ينص القانون على خلاف ذلك، فإن استخدام العميل المستمر لأي من الخدمات أو قنوات الاتصال المذكورة أعلاه بعد إخطاره بإجراءات الأمان المحدثة يشكل موافقة العميل على هذه الإجراءات الأمنية المحدثة. تغطي إجراءات الأمان هذه ما يلي:

A. Authentication Methods

أ. أساليب المصادقة

B. Customer Responsibilities

ب. مسؤوليات العملاء

C. Data Integrity and Secured Communications

ج. سلامة البيانات والاتصالات الآمنة

D. Security Manager and Related Functions

د. مدير الأمن والوظائف ذات الصلة

2. Authentication Methods

2. أساليب المصادقة

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.

تتضمن إجراءات الأمان بعض أساليب المصادقة الآمنة ("أساليب المصادقة") التي تُستخدم لتحديد هوية العميل والتحقق منها بشكل فريد و / أو أي من مستخدميه المصرح لهم من قِبل العميل بشكل نموذجي من خلال آلية واحدة أو مجموعة من الآليات مثل أزواج معرف المستخدم/ كلمات المرور والشهادات الرقمية والقياسات الحيوية ورموز الأمان (التي يتم نشرها عبر الأجهزة أو البرامج) و / أو التحقق من الختم / التوقيع و / أو الأجهزة المرتبطة بأساليب المصادقة (يُشار إليها إجمالاً بـ "بيانات الاعتماد"). تسمح أساليب المصادقة ووثائق التفويض ذات الصلة للبنك بالتحقق من أصل الاتصالات التي يتلقاها البنك.

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.

يمكن الوصول إلى المزيد من المعلومات حول أساليب المصادقة للوصول إلى الخدمات و / أو قنوات الاتصال على CitiDirect® تسجيل الدخول المساعدة الموقع الإلكتروني. يجوز للعميل في أي وقت تحديد أسلوب المصادقة المتاح. أثناء تنفيذ الخدمات أو قنوات الاتصال، يجوز للبنك إعداد أسلوب مصادقة افتراضي، والذي يجوز للعميل تغييره في أي وقت إلى أسلوب مصادقة آخر متاح.

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

تتوفر أساليب المصادقة التالية للوصول إلى الخدمات و / أو قنوات الاتصال:

CitiDirect Authentication Methods CitiDirect - أساليب المصادقة	
Biometrics القياسات الحيوية	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. أسلوب مصادقة رقمي يستخدم السمات المادية الفريدة للمستخدم، (مثل بصمة الإصبع والتعرف على الوجه)، وتقنية المقاييس الحيوية المدمجة على جهاز المستخدم المحمول، وتقنيات التشفير للوصول إلى CitiDirect®. لا يتم نقل بيانات السمات المادية إلى البنك عندما يختار المستخدم طريقة المصادقة هذه.
Mobile Token (non-application based) رمز الوصول عبر الهاتف المحمول (غير القائم على التطبيق)	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. طريقة مصادقة رقمية عبر الهاتف المحمول غير مستندة إلى تطبيق (مثل رمز الوصول عبر الهاتف المحمول بدون تطبيق)، والتي تستخدِم مفاتيح التشفير ووسائل التحقق البيومترية (مثل بصمة الإصبع والتعرُّف على الوجه) لربط جهاز الهاتف المحمول للمستخدم بحسابه لدى CitiDirect من خلال متصفِّح الهاتف المحمول الخاص بالمستخدم. لا تُنقَل بيانات السمات الجسدية (الخصائص البيولوجية) إلى البنك عند اختيار المستخدم طريقة المصادقة هذه. تُسهِم هذه الطريقة في تفعيل المصادقة متعددة العوامل من خلال التحقُّق من هوية المستخدم باستخدام جهازه المحمول المُسجَّل.
Challenge Response Token رمز "استجواب – إجابة"	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. إما (1) رمز مرن قائم على تطبيق الهاتف المحمول (مثل MobilePASS) أو (2) رمز مادي (مثل بطاقة Vasco، SafeWord)، والذي يُستخدم في كل حالة لإنشاء كلمة مرور ديناميكية بعد المصادقة باستخدام رقم تعريف شخصي (مثل رقم التعريف الشخصي PIN المكون من 4 أرقام). عند الوصول إلى CitiDirect®، يقوم النظام بإنشاء استجواب ويتم إنشاء رمز مرور إجابة بواسطة الرمز المميز المستخدم وإدخاله في النظام. تؤدي طريقة المصادقة هذه، عند دمجها مع كلمة مرور آمنة، إلى مصادقة متعددة العوامل.

CitiDirect Authentication Methods CitiDirect - أساليب المصادقة	
One-Time Password Token رمز كلمة المرور المستخدمة لمرة واحدة	Either (i) a mobile application soft token (e.g. MobilePASS) or (ii) a physical token (e.g. SafeWord Card, Vasco) that is used to generate a dynamic password after authenticating with a PIN (e.g. 4-digit PIN). This dynamic password is entered into the system to gain access. إما (1) رمز مرن قائم على تطبيقات الهاتف المحمول (مثل MobilePASS)؛ أو (2) رمز مادي (مثل بطاقة Vasco، SafeWord)، والذي يُستخدم لإنشاء كلمة مرور ديناميكية بعد المصادقة باستخدام رقم التعريف الشخصي (مثل رقم التعريف الشخصي PIN المكون من 4 أرقام). يتم إدخال كلمة المرور الديناميكية في النظام للوصول.
Secure Password كلمة مرور آمنة	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. يقوم المستخدم بإدخال كلمة المرور الآمنة الخاصة به للوصول إلى النظام. عادةً ما تحد كلمة المرور الآمنة من قدرات المستخدم على النظام، على سبيل المثال، فقط من خلال السماح للمستخدم بعرض معلومات معينة. ينتج عن طريقة المصادقة هذه، عند دمجها مع رمز "استجواب - إجابة"، مصادقة متعددة العوامل.
SMS One-Time Code رمز يستخدم لمرة واحدة يرسل عبر الرسائل النصية القصيرة sms	A dynamic password delivered to users via SMS, after which the user enters the dynamic password and a secure password to gain access to the system. كلمة مرور ديناميكية يتم تسليمها للمستخدمين عبر الرسائل النصية القصيرة، وبعد ذلك يقوم المستخدم بإدخال كلمة المرور الديناميكية وكلمة مرور آمنة للوصول إلى النظام.
Voice One-Time Code رمز الصوت لمرة واحدة	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. كلمة مرور ديناميكية يتم تسليمها للمستخدمين عبر مكالمة صوتية آلية، وبعد ذلك يقوم المستخدم بإدخال كلمة المرور الديناميكية وكلمة مرور آمنة للوصول إلى النظام.
Digital Certificates الشهادات الرقمية	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. الشهادة الرقمية هي هوية إلكترونية صادرة عن سلطة الشهادات المعتمدة للمصادقة والتفويض. قد تُنسب الشهادات الرقمية إلى الكيانات القانونية للشركات ("أختام الشركات") أو الأفراد ("الشهادات الشخصية"). يتحمل العميل مسؤولية التحقق الصحيح من هوية جميع مستخدمي الشهادات الشخصية الذين يتصرفون نيابة عن العميل وفقًا للقانون المحلي. يُطلب من البنك والعميل استخدام الشهادات الرقمية المقدمة من الأشخاص المفوضين، لضمان تشفير وحماية جميع الاتصالات المتبادلة عبر اتصال إنترنت عام أو بخلاف ذلك اتصال إنترنت غير آمن.

CitiConnect for Files Authentication Methods CitiConnect للملفات - أساليب المصادقة	
Digital Certificates الشهادات الرقمية	See description above. انظر الوصف أعلاه.
IP Address Whitelist When Using CitiConnect القائمة البيضاء لعنوان بروتوكول الإنترنت عند استخدام 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. قد تعتمد أيضًا بعض اتصالات الإنترنت التي يتلقاها البنك، على سبيل المثال، عبر شبكة افتراضية خاصة (VPN)، على الأطراف التي تتبادل المعلومات باستخدام عناوين بروتوكول الإنترنت (IP) المتفق عليها مسبقًا. لن يقبل البنك سوى الاتصالات الناشئة من عنوان الـ بروتوكول الإنترنت المخصص للعميل، والعكس صحيح؛ وسيقوم البنك فقط بإرسال الاتصالات إلى عنوان الـ بروتوكول الإنترنت المخصص للعميل، والعكس صحيح. تستخدم بالاقتران مع أسلوب الشهادة الرقمية الوارد أعلاه.

CitiConnect API Authentication Methods CitiConnect API - أساليب المصادقة	
Digital Certificates الشهادات الرقمية	See description above. انظر الوصف أعلاه.
IP Address Whitelist When Using CitiConnect القائمة البيضاء لعنوان بروتوكول الإنترنت عند استخدام CitiConnect	See description above. انظر الوصف أعلاه.

CitiConnect for SWIFT Authentication Methods CitiConnect for SWIFT - أساليب المصادقة	
Digital Certificates الشهادات الرقمية	See description above. Can be used in conjunction with SWIFT Authentication method below. انظر الوصف أعلاه. يمكن استخدامه مع أسلوب مصادقة SWIFT الوارد أدناه.

CitiConnect for SWIFT Authentication Methods CitiConnect for SWIFT - أساليب المصادقة	
SWIFT Authentication مصادقة سويفت SWIFT	Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWiFT's Contractual Documentation (as amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications. The Bank is not responsible for any errors or delays in the SWIFT system. The Customer is responsible for providing communications to the Bank in the format and type required and specified by SWIFT. Transmissions and Communications sent or received via SWIFT facilities are subject to SWIFT rules and regulations in effect, including membership rules. The Customer is responsible for being familiar with and conforming to SWIFT messaging standards. ستتم المصادقة على الاتصالات المرسلة بين البنك والعميل عبر شبكة SWIFT، بما في ذلك، على سبيل المثال لا الحصر، معلومات الحساب وأوامر الدفع وتعليمات تعديل أو إلغاء هذه الطلبات باستخدام الإجراءات المحددة في وثائق SWIFT التعاقدية (بصيغتها المعدلة أو المكملة من وقت لآخر) والتي تشمل على سبيل المثال لا الحصر الشروط والأحكام العامة ووصف خدمة FIN أو على النحو المنصوص عليه في الشروط والأحكام الأخرى التي قد تضعها SWIFT. البنك ليس ملزماً بفعل أي شيء بخلاف ما هو وارد في إجراءات SWIFT لإثبات المرسل وصحة هذه الاتصالات. البنك غير مسؤول عن أي أخطاء أو تأخيرات في نظام SWIFT. يتحمل العميل مسؤولية توفير الاتصالات للبنك بالصيغة والنوع المطلوبين والمحددين بواسطة SWIFT. تخضع عمليات النقل والاتصالات المرسلة أو المستلمة عبر مرافق SWIFT لقواعد وأنظمة SWIFT المعمول بها، بما في ذلك قواعد العضوية. يتحمل العميل مسؤولية التعرف على معايير المراسلة لدى SWIFT والامتثال لها.

SWIFT Authentication Method سويفت SWIFT - أساليب المصادقة	
SWIFT Authentication (Direct Connection for Financial Institutions) مصادقة سويفت SWIFT (اتصال مباشر للمؤسسات المالية)	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. ستتم المصادقة على الاتصالات المرسلة بين البنك والعميل عبر شبكة SWIFT، بما في ذلك، على سبيل المثال لا الحصر، معلومات الحساب وأوامر الدفع وتعليمات تعديل أو إلغاء هذه الطلبات باستخدام الإجراءات المحددة في وثائق SWIFT التعاقدية (بصيغتها المعدلة أو المكملة من وقت لآخر) والتي تشمل على سبيل المثال لا الحصر الشروط والأحكام العامة ووصف خدمة FIN أو على النحو المنصوص عليه في الشروط والأحكام الأخرى التي قد تضعها SWIFT. البنك ليس ملزماً بفعل أي شيء بخلاف ما هو وارد في إجراءات SWIFT لإثبات المرسل وصحة هذه الاتصالات. البنك غير مسؤول عن أي أخطاء أو تأخيرات في نظام SWIFT . يتحمل العميل مسؤولية توفير الاتصالات للبنك بالصيغة والنوع المطلوبين والمحددين بواسطة SWIFT. تخضع عمليات النقل والاتصالات المرسلة أو المستلمة عبر مرافق SWIFT لقواعد وأنظمة SWIFT المعمول بها، بما في ذلك قواعد العضوية. يتحمل العميل مسؤولية التعرف على معايير المراسلة لدى SWIFT والامتثال لها.

Digital/Electronic Signature Authentication Methods for Electronic Document Submission التوقيع الرقمي/ الإلكتروني - أساليب المصادقة لتقديم المستندات الإلكترونية	
Digital Signature التوقيع الرقمي	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. نوع من التوقيع الإلكتروني الذي يعزز الشهادات الرقمية للتحقق من صحة وسلامة التوقيع أو الرسالة أو البرنامج أو المستند الرقمي.

Digital/Electronic Signature Authentication Methods for Electronic Document Submission التوقيع الرقمي/ الإلكتروني - أساليب المصادقة لتقديم المستندات الإلكترونية	
Electronic Signature التوقيع الإلكتروني	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. رمز إلكتروني مرفق بعقد أو سجل آخر، فريد ويستخدم من قبل شخص بقصد التوقيع. يمكن إنشاء التوقيعات الإلكترونية في شكل كلمات أو أحرف أو أرقام أو رموز أو النقر فوق زر على موقع ويب أو تحميل فاكس أو مسح التوقيع المادي أو التوقيع على شاشة تعمل باللمس أو الموافقة على أي شروط وأحكام باستخدام الوسائل الإلكترونية. تم إنشاؤها تحت السيطرة الحصرية للشخص الذي يستخدمها، وهي مرفقة منطقياً برسالة بيانات أو مترابطة بها، وقادرة على تحديد الشخص الذي وافق على رسالة البيانات والتصديق على موافقة الشخص. سيتم تقديم هذا التوقيع الإلكتروني إلى البنك من خلال القنوات الإلكترونية للبنك وامتثالًا لطرق المصادقة ذات الصلة الموضحة أعلاه.

Manual Initiated Funds Transfer (MIFT) Authentication Method طريقة مصادقة تحويل الأموال التي يتم بدؤها يدويا (MIFT)	
MIFT Authentication مصادقة MIFT	Manually Initiated Funds Transfer (MIFT), including amendments, recalls, or cancellations of previous manual instructions, may be made by fax or letter or upload to CitiDirect. Not all forms are supported in all countries. Initiators are persons designated by the Customer who are authorized to initiate transactions in accordance with restrictions, if any, are identified by the Customer. Confirmers are person designated by the Customer that Bank may call back, at its discretion, for confirmation of manually initiated instructions for funds transfers. In certain countries, mobile telephone numbers are not accepted as call back numbers. Further details are provided in the applicable Country Cash Management User Guide, Global Manual Transaction Authorization or Universal Nomination Form. MIFT is to be used by the Customer as a contingency method to communication instructions to the Bank. يمكن بدء إجراء تحويل الأموال يدويًا (MIFT)، بما في ذلك التعديلات أو الاستدعاءات أو الإلغاء للتعليمات اليدوية السابقة، عن طريق الفاكس أو الخطاب أو رفعه على CitiDirect®. لا يتم دعم جميع النماذج في جميع البلدان. البادئون هم الأشخاص المعينين من قبل العميل والمصرح لهم ببدء المعاملات وفقًا للقيود، إن وجدت، التي يحددها العميل. يتم تعيين المثبتون من قِبل العميل والتي قد يقوم البنك بالاتصال بهم، وفقًا لتقديره، لتأكيد التعليمات التي تم بدئها يدويًا لتحويل الأموال. في بعض البلدان، لا يتم قبول أرقام الهواتف المحمولة كأرقام اتصال. يتوفر المزيد من التفاصيل في دليل المستخدم لإدارة النقد المعمول به في بلدك أو تفويض المعاملات اليدوية العالمية أو نموذج التعيين الشامل. يجب أن يستخدم العميل MIFT كأسلوب طارئ لإبلاغ التعليمات إلى البنك.

Mail, Fax, Email and Messenger Authentication Methods البريد والفاكس والبريد الإلكتروني وبرنامج المراسلة - أساليب المصادقة	
Seal Image Verification التحقق من صورة الختم	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. يتم التحقق من المراسلات التي يتلقاها البنك عن طريق الفاكس أو البريد أو البريد الإلكتروني أو برنامج المراسلة، باستثناء طلبات MIFT، وتجميعها مع الحرص الواجب استنادًا إلى صورة الختم الواردة في مستند تفويض العميل أو مستند مشابه مقدم إلى البنك.
Signature Verification التحقق من التوقيع	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. يتم التحقق من المراسلات التي يتلقاها البنك عبر الفاكس أو البريد أو البريد الإلكتروني أو برنامج المراسلة، باستثناء طلبات MIFT، بناءً على المعلومات الواردة في مستند تفويض العميل أو مستند مشابه مقدم إلى البنك.
Secure PDF ملف PDF آمن	Encrypted emails are delivered to a regular mailbox as PDF documents that are opened by entering a private password. Both the message and body and any attached files are encrypted. A private password can be set up upon receipt of the first secure email received. يتم تسليم رسائل البريد الإلكتروني المشفرة إلى صندوق بريد عادي كمستندات PDF يتم فتحها بإدخال كلمة مرور خاصة. يتم تشفير كل من نص الرسالة وأي ملفات مرفقة. يمكن إعداد كلمة مرور خاصة عند استلام أول بريد إلكتروني آمن تم استلامه.
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 though encrypted TLS tunnel created by the connection. ينشئ أمان طبقات النقل الإلزامي (Mandatory Transport Layer Security (MTLS ما يمكن أن يكون اتصال بريد إلكتروني خاص وآمن بين البنك والعميل. يتم إرسال رسائل البريد الإلكتروني المرسلة باستخدام هذه القناة عبر الإنترنت من خلال قناة TLS المشفرة التي تم إنشاؤه من خلال الاتصال.

Phone Authentication Methods طرق المصادقة الهاتفية	
PIN رقم التعريف الشخصي (PIN)	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. يُطلب من العملاء الذين يتصلون بالبنك عبر الهاتف إدخال رقم التعريف الشخصي PIN للتحقق من الوصول المصرح به.
Verification Questions أسئلة التحقق	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. يُطلب من العملاء الذين يتصلون بالبنك عبر الهاتف من قبل ممثلي خدمة البنك تقديم ردود شفوية صحيحة على أسئلة التحقق من أجل التحقق من الوصول المصرح به.

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

يختلف توفر طرق المصادقة الموضحة أعلاه بناء على الأسواق المحلية.

3. Customer Responsibilities

3. مسؤوليات العملاء

3.1 Identifying Authorized Users: Customer is responsible for identifying: (i) all individuals acting on the authenticate the Customer's 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.

3-1 تحديد المستخدمين المصرح لهم: يتحمل العميل مسؤولية تحديد: (1) جميع الافراد الذين يتصرفون نيابة عن العميل في الحساب (الحسابات) على مستوى المؤسسة لجميع الخدمات وقنوات الاتصال، و (2) كل شخص يتصرف نيابة عن العميل مفوض حسب الأصول من قبل العميل للتصرف على حساب العميل.

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.

3-2 يتحمل العميل مسؤولية تعيين ومراقبة أي حدود للمعاملات يتم تعيينها للعميل و / أو مستخدميه والتأكد من أن هذه الحدود (أ) لا تتجاوز الحدود كما هو مطلوب بموجب السياسات الداخلية للعميل وغيرها من الوثائق التأسيسية السلطات الاخرى مثل قرارات مجلس إدارة العميل، أو تفويضات البنك ،أو التوكيل الرسمي أو ما يعادلها، و(ب) تنعكس بشكل صحيح على جميع قنوات الاتصال واستحقاقات المستخدم.

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.

3-3 قد تتطلب بعض السلطات القضائية تحديد الأفراد (وبيانات الاعتماد الخاصة بهم) من قبل البنك وفقًا لمتطلبات تشريعات مكافحة غسل الأموال المعمول بها قبل منح حق الوصول لأداء وظائف معينة. يرجى الاتصال بممثل خدمة العملاء الخاص بك أو زيارة موقع CitiDirect® لمزيد من المعلومات.

3.4 Safeguarding of Authentication Methods

3-4 حماية طرق المصادقة

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.

يتحمل العميل مسؤولية حماية أساليب المصادقة وبيانات الاعتماد بأعلى مستوى من العناية والاجتهاد، وضمان أن الوصول إلى بيانات الاعتماد وتوزيعها يقتصر فقط على الأشخاص الذين أذن لهم العميل. المراسلات من الطرف الثالث: عندما يستخدم العميل بيانات اعتماد لتحديد اتصالاته والمصادقة عليها باعتبارها صادرة منه ككيان قانوني، فإن العميل مسؤول عن ممارسة السيطرة الكاملة على استخدام بيانات الاعتماد هذه عند إرسال المراسلات إلى البنك، بما في ذلك حيث يتم إرسال هذه الاتصالات عن طريق التطبيقات و / أو الأنظمة التي يديرها طرف ثالث نيابة عن العميل. في جميع الأحوال، البنك (أ) سيعتبر أي اتصال يتلقاه من خلال قناة اتصال إلكترونية، والذي يتم استلامه من قبل البنك وفقًا لإجراءات الأمان هذه مصدق عليه رسمياً على أنه صادر من العميل، كاتصال يصدر العميل تعليمات به و (ب) يجوز له التصرف بناءً على أي اتصال يتلقاه نيابة عن العميل وفقًا لإجراءات الأمان هذه.

4. Data Integrity and Secured Communications

4. سلامة البيانات والاتصالات الآمنة

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.

4-1 سيقوم «العميل» بنقل البيانات والتواصُل وتبادل «المراسلات» مع البنك عبر الإنترنت و/أو البريد العادي و/أو البريد الإلكتروني و/أو الفاكس، مع علمه بأنَّ هذه الوسائل (1) ليست بالضرورة وسائل تواصُل وتسليم آمنة، و(2) لا تخضع لسيطرة البنك. كما يُدرك «العميل» أنَّه إذا كان مستخدمو «العميل» مخوَّلين بالوصول إلى «الخدمات المصرفية المفتوحة» و/أو منصَّات مشابهة تابعة لجهات خارجية (أطراف ثالثة) خارج أنظمة Citi، فقد تُنقَل بيانات «العميل» عبر هذه المنصَّات التابعة لجهات خارجية (أطراف ثالثة) والتي لا تخضع لسيطرة البنك.

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.

4-2 يستخدم البنك أساليب التشفير الرائدة في الصناعة (على النحو الذي يحدده البنك)، والتي تساعد على ضمان الحفاظ على سرية المعلومات وعدم تغييرها أثناء النقل الإلكتروني.

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.

4-3 إذا اشتبه العميل أو أصبح على علم بوجود عطل فني أو أي وصول غير لائق أو محتمل إلى خدمات البنك أو قنوات الاتصال أو طرق المصادقة أو استخدامها من قبل أي شخص (سواء كان شخصًا مصرحًا له أم لا)، فيجب على العميل إخطار البنك بحدوث ذلك. في حالة الوصول أو الاستخدام غير اللائق أو الاحتيالي من قبل شخص مصرح له، يجب على العميل اتخاذ إجراءات فورية لإنهاء وصول هذا الشخص المصرح له إلى خدمات البنك أو قنوات الاتصال واستخدامها.

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.

4-4 إذا كان العميل يستخدم تنسيق الملفات أو برنامج التشفير (سواء تم توفيره من قبل البنك أو طرف ثالث) لدعم تنسيق البيانات والتعليمات الخاصة بالعميل والاعتراف بها والتصرف بموجب الاتصالات مع البنك، فسيستخدم العميل هذه البرامج فقط من أجل الغرض الذي تم تثبيته من أجله.

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.

5-4 يوافق العميل على أنه يجوز للبنك تعليق أو رفض وصول المستخدمين إلى الخدمات التي تتطلب استخدام بيانات الاعتماد (1) في حالة الاشتباه في الاستخدام غير المصرح به أو الاحتيالي لبيانات الاعتماد و / أو (2) لحماية الخدمات أو بيانات الاعتماد.

5. Security Manager and Related Functions

5. مدير الأمن والوظائف ذات الصلة

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:

بالنسبة للتطبيقات التي يمكن الوصول إليها في CitiDirect® (باستثناء الشهادات الشخصية الموضحة أدناه)، يطلب البنك من العميل إنشاء وظيفة "مدير الأمن". ومديرو الأمن مسؤولون عن:

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);

5-1 إنشاء والإبقاء على إمكانية الوصول واستحقاقات المستخدمين (بما في ذلك مديري الأمن أنفسهم) بما في ذلك الأنشطة مثل: (أ) إنشاء أو حذف أو تعديل ملفات تعريف المستخدمين (بما في ذلك ملفات تعريف مدير الأمن) وحقوق الاستحقاق (لاحظ أن اسم المستخدم يجب أن يتطابق مع وثائق الهوية الداعمة) ؛ (ب) إنشاء ملفات تعريف الوصول التي تحدد الوظائف والبيانات المتاحة للمستخدمين الفرديين ؛ (ج) تمكين وتعطيل بيانات اعتماد تسجيل دخول المستخدم ؛ و (د) تعيين حدود المعاملات (لاحظ أن هذه الحدود لا يتم مراقبتها أو التحقق من صحتها من قبل البنك ويجب على العميل مراقبة هذه الحدود للتأكد من أنها تتوافق مع السياسات والمتطلبات الداخلية للعميل، بما في ذلك على سبيل المثال لا الحصر، تلك التي وضعها مجلس الإدارة بشأن العميل أو ما يعادلها)؛

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;

5-2 إنشاء وتعديل الإدخالات في المكتبات التي يحتفظ بها العملاء (مثل الدفعات بالصيغ المعدة مسبقا والمكتبات المستفيدة) وتفويض المستخدمين الآخرين للقيام بنفس الشيء؛

5.3 Modifying payment authorization flows;

5-3 تعديل تدفقات إذن الدفع؛

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

5-4 تخصيص بيانات اعتماد كلمة المرور الديناميكية أو غيرها من بيانات اعتماد الوصول إلى النظام أو كلمات المرور لمستخدمي العميل؛

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

5-5 إخطار البنك، إذا كان هناك أي سبب للشك في تعرض الأمن للخطر؛ و

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

6-5 إدارة وشراء الشهادات الرقمية وتفويض المستخدمين الآخرين بالقيام بالمثل.

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.

يرجى الملاحظة: قد تختلف أدوار ومسؤوليات مدير الأمن أو لا تكون قابلة للتطبيق في أسواق معينة بسبب المتطلبات التنظيمية و / أو القدرات التشغيلية. في مثل هذه الأسواق، قد يطلب البنك وثائق إضافية ومعلومات أخرى من العميل لأداء وظائف مدير الأمن نيابة عن العميل.

6. Use of CitiDirect and CitiConnect by Security Managers

6. استخدام CitiDirect وCitiConnect من قبل مديري الأمن

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.

يطلب البنك شخصين (2) منفصلين لإدخال التعليمات والإذن بها ؛ لذلك، مطلوب ما لا يقل عن اثنين من مديري الأمن. يمكن لأي إثنين من مديري الأمن، يعملان بتنسيق وانسجام، إعطاء تعليمات و / أو تأكيدات من خلال قنوات الاتصال فيما يتعلق بأي وظيفة مدير أمن أو فيما يتعلق بتسهيل الاتصالات. سيتم قبول أي من هذه الاتصالات، عندما يأذن بها مديران أمن، والتصرف من قبل البنك واعتبار أنه تم إعطائها من قبل العميل. يوصي البنك بتعيين ثلاثة مديري أمن على الأقل لضمان النسخ الاحتياطي الكافي. يجب على العميل تعيين مديري أمن العميل في استمارة التحاق بقنوات حلول الخزانة والتجارة. يجوز أيضًا لمدير الأمن الخاص بالعميل أن يعمل كمدير أمن لكيان طرف ثالث (على سبيل المثال، تابع للعميل) ويمارس جميع الحقوق المتعلقة به (بما في ذلك تعيين المستخدمين لحساب (حسابات) كيان الطرف الثالث)، بدون أي تعيين إضافي، إذا نفذ ذلك الكيان التابع لطرف ثالث نموذج سلطة الوصول الشامل (أو أي شكل آخر من أشكال التفويض المقبول للبنك) يمنح العميل حق الوصول إلى حسابه (حساباته). ينطبق هذا فقط فيما يتعلق بالحسابات التي يغطيها التفويض ذي الصلة.

7. Use of CitiDirect by Security Officers (For Personal Certificates only)

7. استخدام CitiDirect من قبل ضباط الأمن (للشهادات الشخصية فقط)

The Bank requires two (2) separate individuals to manage digital certificates attributed to individuals ("Personal Certificates"). Therefore, two Security Officers are required to assign and remove Personal Certificates to users, for the purpose of authenticating and authorizing Communications on the connectivity channels. The Bank recommends the designation of at least three Security Officers to ensure adequate backup. Any Communications authorized by Personal Certificates will be accepted and acted on by the Bank and deemed to be given by the Customer.

يطلب البنك شخصين (2) منفصلين لإدارة الشهادات الرقمية المنسوبة إلى الأفراد ("الشهادات الشخصية"). لذلك، يلزم عدد إثنين موظفي أمن لتخصيص وإلغاء الشهادات الشخصية للمستخدمين، بغرض المصادقة على الاتصالات والإذن بها على قنوات الاتصال. يوصي البنك بتعيين ثلاثة موظفي أمن على الأقل لضمان النسخ الاحتياطي الكافي. سيتم قبول أي اتصالات مصرح بها من خلال الشهادات الشخصية والتصرف من قبل البنك واعتبار أنه تم إعطائها من قبل العميل.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions