Security Procedures

1. Introduction

These "Security Procedures", as referenced in the Communications section of the Master Account and Service Terms ("MAST") (or other applicable account terms and conditions), are designed to authenticate the Customer's log-on to the Bank's connectivity channels and to verify the origination of Communications between Bank and Customer in connection with the following Services or connectivity channels (the availability of which may vary across local markets).

- CitiDirect® (including WorldLink®)
- CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
- Interactive Voice Response ("IVR")
- Email/Fax/Mail/Messenger/Phone with the Bank
- Other local electronic connectivity channels

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:

A. Authentication Methods

B. Customer Responsibilities

C. Data Integrity and Secured Communications

D. Security Manager and Related Functions

2. Authentication Methods

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.

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.

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

CitiDirect Authentication Methods	
Biometrics	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.
Mobile Token (non-application based)	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.
Challenge Response Token	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.
One-Time Password Token	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.
Secure Password	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.
SMS One-Time Code	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.
Voice One-Time Code	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.
Digital Certificates	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.

CitiConnect for Files Authentication Methods	
Digital Certificates	See description above.
IP Address Whitelist When Using 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.

CitiConnect API Authentication Methods	
Digital Certificates	See description above.
IP Address Whitelist When Using CitiConnect	See description above.

CitiConnect for SWIFT Authentication Methods	
Digital Certificates	See description above. Can be used in conjunction with SWIFT Authentication method below.
SWIFT Authentication	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.

SWIFT Authentication Method	
SWIFT Authentication (Direct Connection for Financial Institutions)	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.

Digital/Electronic Signature Authentication Methods for Electronic Document Submission	
Digital Signature	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document.
Electronic Signature	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.

Manual Initiated Funds Transfer (MIFT) Authentication Method	
MIFT Authentication	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.

Mail, Fax, Email and Messenger Authentication Methods	
Seal Image Verification	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.
Signature Verification	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.
Secure PDF	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.
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.

Phone Authentication Methods	
PIN	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access.
Verification Questions	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.

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

3. Customer Responsibilities

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.

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.

3.3 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.

3.4 Safeguarding of Authentication Methods

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.

4. Data Integrity and Secured Communications

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.

4.2 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.

4.3 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.

4.4 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.

4.5 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. Security Manager and Related Functions

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:

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);

5.2 Creating and modifying entries in Customer maintained libraries (such as preformatted payments and beneficiary libraries) and authorizing other users to do the same;

5.3 Modifying payment authorization flows;

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

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

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

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.

6. Use of CitiDirect and CitiConnect by Security Managers

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.

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

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.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions