citi

Security Managers Designation

Client Name:
Client Address:

Country: **Zip:**
Phone No: **Fax No:**

Client acknowledges that the method by which it will be transmitting data to and otherwise exchanging communications with Citibank and its affiliates and subsidiaries (the “Bank”) utilizes the Internet. Client understands and acknowledges the security procedures for communications described in the attached document, and agrees that Bank may act on instructions received in compliance with such procedures (as such procedures may be updated and advised to Client by electronic means or otherwise from time to time). Client further understands and acknowledges the roles and responsibilities of its Security Managers and Users as set forth in the attached document, and hereby appoints the persons whose details are set forth below as its Security Managers.

Primary Security Manager Name Phone Email	**Alternate Security Manager** Name Phone Email
Specimen Signature □ **New** □ **Delete**	**Specimen Signature** □ **New** □ **Delete**

Alternate Security Manager Name Phone Email	**Alternate Security Manager** Name Phone Email
Specimen Signature □ **New** □ **Delete**	**Specimen Signature** □ **New** □ **Delete**

^ applies to Corporate Internet Banking only

Signed For and Behalf of

Corporate Seal & Stamp(법인 인감 & 명판)

Date

February, 2012

CitiDirect® Online Banking Security Procedures (Cash and Trade)

CitiDirect Security Managers (minimum of two (2) required)

CitiDirect requires **two** separate individuals to input and authorize instructions; therefore, a minimum of two Security Managers is required. Any two Security Managers, acting in concert, are able to give instructions and/or confirmations through CitiDirect in relation to any Security Manager function or in connection with facilitating your communication with Bank via the Internet.

The roles and responsibilities of the Client's Security Managers include:

(i) appointing additional Security Managers (including any Security Managers employed by entities other than the Client);

(ii) allocating dynamic password cards or other system access cards or passwords to the Client's users ("Users", which Users may include, among others, the Security Managers themselves and persons employed by entities other than the Client, in each case as designated by the Security Managers);

(iii) appointing and managing the access and entitlements of the Users, including such activities as (A) creating, deleting or modifying User profiles and entitlement rights, (B) building access profiles that define the applications available to various Users, and (C) enabling and disabling User identification;

(iv) defining and administering product setup and site/flow control, such as identifying levels of transaction authorization and modifying payment authorization flows;

(v) notifying Bank if there is any reason to suspect that security has been compromised;

(vi) creating, deleting or modifying Client-managed libraries (such as preformatted payments and beneficiary libraries), and authorizing other Users to do the same; and

(vii) where relevant, completing, amending, approving and/or supplementing such Client implementation forms as may be reasonably requested by Bank from time to time in connection with the provision of services and/or products to Client.

As noted above, Security Managers have the ability to assign transaction limits to Users for those Citigroup products to which such Users have access. These limits are not monitored or validated by Bank; Client is responsible for monitoring these limits and ensuring compliance with Client's internal policies and requirements, including but not limited to those established by the Client's Board of Directors or equivalent. Users who are permitted to input and/or authorize payments may have the ability to accept FX rates if such is an integral part of a payment service that Client has opted to access through CitiDirect.

All activities of Security Managers and Users can be viewed using the CitiDirect Audit Reports feature.

SafeWord™ Authentication Method

Security Managers and all Users who want to initiate or approve transactions (and whose User Profile permits them to do so) must use the SafeWord Authentication method.

SafeWord Authentication involves the use of a SafeWord card. The SafeWord card is a physical hardware device that is used in conjunction with the challenge/response prompt inquiry that appears on the CitiDirect Sign-On screen each time a User logs on to CitiDirect. In order to use the SafeWord card, the User must enter the proper Personal Identification Number (PIN) into the card. After the proper PIN is entered and the User enters the challenge that appears on the CitiDirect Sign-On screen, the SafeWord card will generate a dynamic password. When this dynamic password is entered into the response field on the CitiDirect Sign-On screen, the User will have access to the CitiDirect functions assigned to the User in his/her User profile.

Secured Password with Risk Based Authentication Method

The Secured Password with Risk Based Authentication Method is available on an approved exception basis by Citibank only to Users who have access to reporting, inquiry/ netting input and reporting functions. The Secured Password with Risk Based Authentication Method requires Security Managers to set up Users as Secured Password Users. Security Managers are responsible for the distribution of credentials to Secured Password Users. Secured Password Users must use an ID and Password initially distributed to the Users by Citibank for identification and authentication. In addition, at the point of login if Citibank determines a risk assessment as high, Secured Password Users will be directed to a second level authentication which uses a pre-registered challenge question and response. The challenge questions are selected the first time Secured Password Users log on.

Secured Communications

Corporate Internet Banking sessions between identified and authorized Users and Bank are encrypted through the use of Secure Sockets Layer (SSL) 128-bit encryption.

Note: In some instances (e.g., CitiDirect screens and manuals), “Security Managers” are referred to as “System Administrators”.

Corporate Internet Banking
Security Procedures

Corporate Internet Banking utilizes an ID and PIN to conduct user identification and authentication. Each user authenticates him/herself with a unique ID and PIN. While Bank assigns the initial PIN, the user has the ability to change it.

The appointed Security Managers will be authorized access the accounts and all other accounts held with **Citibank** (also included as the "Bank" thereafter) which are duly authorized by the related entities to access.

Any one of the appointed Security Managers is authorized to give instructions to Bank (and Bank is authorized to accept such instructions) in relation to any activity mentioned in the Corporate Internet Banking Security Managers Designation or in connection with facilitating communication between Bank and Client via the Internet. They will be responsible for the proper distribution of user ID's and Initial Password to new users. They will acknowledge to Bank when these users have changed the initial passwords issued to them.

The Security Manager is allowed to carry out all the following responsibilities singly:

1. Create new Corporate Internet Banking users
2. Delete any Existing Corporate Internet Banking users
3. Modify e-Statement Entitlement
4. Reset/Enable User Passwords
5. Ensure the change the initial passwords issued to users

Corporate Internet Banking sessions between identified and authorized users and Bank are encrypted through the use of Secure Sockets Layer (SSL) 128-bit encryption.

February, 2012