General Descriptive Information – Online Enterprise Banking Services

This document provides you only with general descriptive information relating to the use of Online Enterprise Banking Services ("**Online Enterprise Banking Services**") and it is solely prepared for your reference only. For more details, please refer to:

- the Specific Terms and Conditions for Online Enterprise Banking Services and
- the Terms and Conditions for Accounts and Related Services (For Enterprise Customers); and
- our Website.

1. Customer obligations in relation to security for Online Enterprise Banking Services

- The Customer shall be reminded that any person who gains access to or acquires knowledge of the Customer's Identity Verification Information will be able to access the Online Enterprise Banking Services and give Instructions to the Bank in respect of the Customer's account(s) maintained with the Bank, including but not limited to placing orders, withdrawing or otherwise dealing with the Customer's funds.
- "**Identity Verification Information**" shall mean any one or more of the Customer's User Name, Customer Number, Password, Security Code and (if applicable) Biometric Credentials under the Biometric Credential Authentication Service.
- It is very important for the Customer to take appropriate measures (including, but not limited to those security measures mentioned under the Specific Terms and Conditions for Online Enterprise Banking Services) to safeguard the Identity Verification Information.
- Also, to protect the Customer's privacy and assets, the Customer shall take steps to keep confidential and secure the Customer's Permitted Mobile Device, Passwords, and bank or account related information and to prevent unauthorised use of the Customer's Permitted Mobile Device.
- Customer may refer to the section headed Security Tips for more information.

2. Customer's liability for unauthorized transactions

- The Bank will ensure that before carrying out any Instruction, the Instruction is authenticated by the Bank through checking any one or more of the Customer's Identity Verification Information.
- The Customer shall be solely responsible for using, and shall be liable for any loss that results from any unauthorised use of the Mobile Banking App, the Biometric Credential Authentication Service and/or the Mobile Token due to the Customer's failure to adopt and maintain appropriate safeguards.
- Also, the Customer agrees to hold the Bank, its affiliates and/or its licensees (as applicable) fully indemnified against all losses, damages, costs and expenses (including professional and legal costs) if any person other than the Customer gains access to or acquires knowledge of the Customer's Identity Verification Information.

Important Notice to Customer

- Customers will be liable for all losses if they have acted fraudulently.
- Customers may also be held liable for all losses if they have acted with gross negligence (this may include cases where customers knowingly allow the use by others of their device or authentication factors) or have failed to inform institutions as soon as reasonably practicable after realizing that their authentication factors or devices for accessing the Online Enterprise Banking Services have been compromised, lost or stolen, or that unauthorized transactions have been conducted.
- Customers will be liable for all losses if they fail to follow the safeguards set out below.
    - Customers shall take reasonable steps to keep any device (for example, personal computers, security devices that generate one-time passwords and smart cards that store digital certificates) or authentication factors (for example, passwords and authentication tokens) used for accessing Online Enterprise Banking Services secure and secret.

- Customers have to take reasonable steps to keep the device safe and the authentication factors (for example, passwords) secret to prevent fraud.
- Among others, Customers are advised –

(a) that they should destroy the original printed copy of the passwords;
(b) about the risks associated with the adoption of biometric, soft token (where applicable) or device binding as one of the authentication factors used for initiating relevant transactions (e.g. contactless mobile payments) and the relevant protection measures to secure the devices and authentication factors;
(c) to change the Password and Mobile Token Password (where applicable) on a regular basis
(d) that they should not allow anyone else to use their authentication factors;
(e) never to write down the passwords on any device for accessing Online Enterprise Banking Services or on anything usually kept with or near it;
(f) not to write down or record the passwords without disguising them;
(g) that they should notify the institutions as soon as practicable after they identify unusual or suspicious transactions on their accounts; and
(h) of the need to ensure that their contact details registered with the institutions for the purpose of receiving important notifications from the institutions (for example, SMS and email notifications for online payments) are up-to-date to allow relevant notifications to be delivered to the customers on a timely basis.

3. Security incidents reporting

- In the course of making use of Online Enterprise Banking Services, if the Customer becomes aware or suspects that:
  - any Password has been stolen, lost, disclosed to any unauthorised person or otherwise compromised; or
  - any unauthorised use of an Account or Service is taking or has taken place,

  the Customer must immediately notify the Bank in person or by telephone (+852) 2903 8366 or in such other manner (such as contacting your Relationship Manager) as the Bank may from time to time prescribe.
- The Bank may ask the Customer to confirm any such verbal or telephone notification in writing and, until the Bank's actual receipt of such notification, the Customer shall remain responsible for any and all use of the relevant Account or Service by unauthorised persons or for unauthorised purposes.

4. Fees and charges

- Generally speaking, the Bank does not charge any fee for the use of the Mobile Banking App nor the Website. However, the Customer will be responsible for the charges associated with using the data service on its Mobile Devices or any other electronic devices. The Customer should check with its network operator for details of the usage fees.
- Also, the Customer shall pay all applicable fees and charges (if any) set out in this Schedule of Service Fees (General Banking Services) associated with using the Online Enterprise Banking Services. These fees and charges are set out in full on the Mobile Banking App, the Website and, in addition to these fees (if any), the Bank may also charge fees for other products and services.
- The Bank may deduct any fees from the Customer account(s) maintained with the Bank (where applicable) for using the Online Enterprise Banking Services.

5. Customers' personal data protection

- In providing the Online Enterprise Banking Services, the Bank, its affiliates and/or its licensees (as applicable) may collect personal data relating to the authorised representatives and/or any directors, officers, employees, authorised persons of the Customer (collectively, "**Relevant Persons**") for various purposes, including but not limited to facilitating the Bank's provision of the Online Enterprise Banking Services and promotion of the Bank's other products and services.

- The collection, use, transfer, processing, retention, maintenance and handling of any such personal data by the Bank, its affiliates and/or its licensees, are subject to the Bank's Privacy Policy and PDPO Notice.
- The Customer shall obtain the consent from the Relevant Persons regarding the use of their personal data by the Bank and/or its affiliates and licensees.

In the event of any inconsistency between the English version and the Chinese version of this general descriptive information, the English version will prevail.