Privacy Policy & Security Information For HLB Connect Internet Banking Services

General

All personal data provided to HL Bank Singapore ("HLBS") by you or acquired by HLBS from the public domain, as well as personal data that arise as a result of the provision of the Services to you by HLBS, whether through HLB Connect or otherwise, will be subject to HLBS' Privacy Policy as may be amended from time to time. Copies of HLBS' Privacy Policy are available upon request or from the HLBS website.

Use of Personal Data by HLBS for Marketing Purposes

HLBS may use the personal data which you have provided to offer you products or services, including but not limited to, special offers, promotions, contests or entitlements that may be of interest to you or for which you may be eligible. Such messages may be sent to you in various different modes including but not limited to:

(i) electronic mail;
(ii) direct mailers;
(iii) short message services;
(iv) telephone calls;
(v) facsimile and other mobile messaging services.

In doing so, we will comply with the Personal Data Protection Act (Cap. 362) of Singapore ("PDPA") and other applicable data protection and privacy laws.

By applying for HLB Connect, you are taken to have consented to your personal data being used and disclosed in accordance with HLBS' Privacy Policy as may be amended from time to time.

In respect of sending telemarketing messages to your telephone number via short message service, telephone calls, facsimile and other mobile messaging services, please be assured that we shall only do so if you have provided clear and unambiguous consent in writing or other recorded form to do so or if your registration of that said number with the Do Not Call Registry had not otherwise been effected. If we have an ongoing relationship with you and you have not indicated to us that you do not wish to receive telemarketing messages sent to your telephone number, we may send you telemarketing messages to that said number related to the subject of our ongoing relationship via short message service, facsimile and other mobile messaging services. Please note that you may at any time request that we stop contacting you for marketing purposes via selected or all modes.

Nothing in this section shall vary or supercede the terms and conditions that govern our relationship with you.

Security Measures Adopted to Protect the Information

We protect your information safely in a high security data centre, adhering to stringent security controls, measures and protocols to safeguard the privacy of your information. While we shall use our best efforts to ensure that the privacy of all Information is kept secure, please note that it is an accepted fact that no data transmission conducted over the Internet and/or through other electronic channels can be guaranteed to be wholly secure. As such, please ensure that your information is not accessible or disclosed to anyone. Further thereto, we shall neither be held responsible nor liable for any damages or losses which you may suffer, whether directly or indirectly, as a result of the said Information being stolen, tampered with, copied, abused, misused or

otherwise violated. For further information on our security measures, please refer to our Security Statement below.

Security Statement

We in HLBS will at all times use our best efforts to ensure that all information disclosed, shared, stored or used and any transactions performed by you through HLB Connect internet banking website are kept secure, safe, private and confidential. For this purpose, we have put in place security measures and privacy protection control systems designed to ensure that the security, integrity, privacy and confidentiality of your information and transactions are not compromised.

Username and Password

To control access to our HLB Connect internet banking services, every customer is required to input your username and password. This username and password is the access key to your financial information. To ensure the integrity of your password, you are advised to do the following:-

- Password should be at least 8 digits and should include alphanumeric characters.
- Password should not be based on guessable information such as user-id, personal telephone number, birthday or other personal information.
- Password should be kept confidential and not be divulged to anyone.
- Password should be memorised and not be recorded anywhere.
- Password should be changed regularly or when there is any suspicion that it has been compromised or impaired.
- The same Password should not be used for different websites, applications or services, particularly when they relate to different entities.
- You should not select the browser option for storing or retaining user name and password.

Temporary ID

Customers registering for the first time or resetting HLB Connect are required to input a Temporary ID. This 10-character ID of alphabets and numbers together with your valid Account Number and Identity Card/Passport Number allows you to register or reset HLB Connect and proceed to create or change your Username and Password.

One Time Password

For certain financial transactions, the customer is required to input a One Time Password ("OTP") in order to validate the transaction. The OTP will be issued to your registered mobile phone number with HLBS or your security token. Each OTP is valid for a single transaction only. The OTP should not be revealed nor made accessible to anyone else. You should:

- Not allow anyone to use or tamper with your security token;
- Not reveal the OTP to anyone, even when requested to do so by an authorised officer of HLBS;
- Not divulge the serial number of your security token to anyone;
- Inform HLBS immediately on the loss of your mobile phone or change in your mobile phone number.

Data Privacy, Confidentiality and Integrity

To ensure data privacy, confidentiality and integrity, all information disclosed, shared, stored or used and any transactions performed by you through HLB Connect internet banking website are encrypted using the Secure Sockets Layer secured 256-bit from Verisign Certificate Authority.

System Security and Monitoring

To provide a secured environment for HLB Connect website, HLBS adopts a combination of system security and monitoring measures:

- Firewall systems, strong data encryption, anti-virus protection and round the clock security surveillance systems to detect and prevent any form of illegitimate activities on our network systems.
- Automatic log out of HLB Connect when there is no activity detected for a period of time.
- Disallow access to HLB Connect as may be determined by HLBS at its absolute discretion without any prior notice of such deactivation.
- Regular security reviews are conducted on our systems by our internal System Audit as well as external security experts.
- Collaboration with major vendors/manufacturers to keep abreast of information security technology developments and implement where relevant.

Customer's Responsibilities

At HLBS, we are constantly updating our security technology to protect your privacy and confidentiality, but we do not have control over the electronic devices used by you to access HLB Connect or the mobile phone you use to receive your OTP or such other security codes, which HLBS may issue from time to time.

Please exercise caution and be on the alert for suspicious email or phone call/SMS asking for your personal or banking account related information with the intention of carrying out internet theft and fraud. Never respond to any email or SMS with an internet URL link which further requires you to input online security credential data like username, password and OTP.

It is your responsibility to safeguard your online information and transactions by taking all reasonable measures which may include the following:

- Do not share your information or provide any opportunity for anyone to gain access to your information through your personal electronic devices.
- Always log in to the correct URL (https://hlbankconnect.com.sg/rib/app/fo/login).
- Always log out before visiting other Internet websites or once you have completed your transactions.
- Always ensure that you have the necessary and appropriate security software and firewall installed at your computer, in particular if you are using a wireless internet connection.
- Always update your internet browser when new versions are released because they often include new security features.
- Check your internet browser for built-in safety features that you may or may not elect to use.
- Check the website certificate before log in.
- Always clear your internet cache after you log out from an online session.

- Do not display your account information in a manner visible to others, and your personal computer should never be left unattended.

Non-liability of HLBS

HLBS shall not be liable to you in the following circumstances:

(a) Failure on your part to adhere to the applicable terms and conditions;
(b) Failure to follow recommended security measures as above; and
(c) Failure of HLBS to act on your instructions as a result of anything beyond the control of HLBS. This includes, amongst other things, any machine, equipment, system or software failing to work, failure to act by any third party and any act, omission or delay of any agent or third party. If any loss or damage results directly from HL Bank's security breach, gross negligence, wilful default or fraud then HL Bank will be liable to the customer, and not to any third party, for the amount of any such loss or damage. However, HLBS will not be liable to the customer for any loss of business, loss of reputation, loss of opportunity, loss of profits and any type of special, consequential or indirect loss whatsoever.

-END-