Security Policy

For Hong Leong Bank Connect Digital Banking Services

All personal data provided to HLBB/HLISB by you or acquired by HLBB/HLISB from the public domain, as well as personal data that arises as a result of the provision of the Services to you by HLBB/HLISB, whether through Hong Leong Bank Connect or otherwise, will be subject to the Privacy Policy of HLBB/HLISB as may be amended from time to time. Copies of the Privacy Policy of HLBB/HLISB are available upon request or from the HLBB/HLISB website.

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 Hong Leong Bank Berhad (“HLBB”) and Hong Leong Islamic Bank (“HLISB”) 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 Hong Leong Bank Connect (“HLB Connect”) digital 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 digital 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:-

- When choosing a password, do not choose one that can be easily guessed by other person(s).

- Avoid using personal information such as your name, birth date, telephone number or words listed in a standard dictionary.
- Memorize your password and do not write it down.
- The password should never be revealed nor made accessible to anyone. It should not be disclosed even when requested to do so by an authorised officer of HLBB/HLISB.
- For your further protection, you are encouraged to change your password from time to time.
- If you have forgotten your password, you may reset your HLB Connect.

ATM PIN

Customers using the ATM or Debit Card mode of first-time registration or reset HLB Connect are required to input their ATM PIN. This 6-digit ATM PIN together with your active ATM/Debit Card Number and Identity Card/Passport Number allows you to register or reset HLB Connect and proceed to create or change your Username and Password.

Card PIN

Customers using the Credit Card mode of first-time registration or reset HLB Connect are required to input their Card PIN. This 6-digit Card PIN together with your active Credit Card Number and Identity Card/Passport Number allows you to register or reset HLB Connect and proceed to create or change your Username and Password.

Temporary ID

Customers using the Account Number mode of first-time registration or reset HLB Connect are required to input a Temporary ID. This 10 characters 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.

The Temporary ID can be requested via any HLBB/HLISB’s branches

The Temporary ID is valid for three (3) days and can only be used once.

Transaction Authorisation Code

For certain financial transactions, the customer is required to request for and input a Transaction Authorization Code (“TAC”) in order to validate the transaction. The TAC will be issued automatically online when you are performing a first-time registration or resetting your HLB Connect or conducting a specific financial transaction. Each TAC is valid for a single transaction only and will expire after 3 minutes. The TAC should not be revealed nor made accessible to anyone else. It should not be disclosed even when requested to do so by an authorised officer of HLBB/ HLISB

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 digital banking website are encrypted using the 256-bit Secure Sockets Layer from Verisign Certificate Authority.

System Security and Monitoring

To provide a secured environment for HLB Connect website, HLBB/HLISB 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.
- The additional use of security picture to confirm access to the correct HLB Connect digital banking website and the identity of the customer.
- Automatic log out of HLB Connect when there is no activity detected for a period of time.
- Disallow access to HLB Connect after 3-months of inactivity
- 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 HLBB/HLISB, 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 TAC or such other security codes, which HLBB/HLISB 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 TAC.

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 opportunities for anyone to gain access to your information through your personal electronic devices.

- Always log in to the correct URL (www.hongleongconnect.my) and that you view the correct security picture on entering your Username.
- Always log out before visiting other Internet sites 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.