Security Policy
For Connect Digital Banking Services

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

Security Measures Adopted to Protect the Information
We protect your information safely in a high security data center, 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 HLBCAM 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 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 Connect digital banking services, every customer is required to input your Username and Password. The Username and Password are 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 authorized officer of HLBCAM.
- 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 Password online by re-registering your Connect services.

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

Temporary ID

In order to register and access our Connect digital banking services for the first time, every customer is 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 Call Center or any Branch/Transaction Office of HLBCAM.
- The Temporary ID should not be written down, revealed nor made accessible to anyone. It should not be disclosed even when requested to do so by an authorized officer of HLBCAM.
- The Temporary ID is valid for three (3) days and can only be used once.

TAC (Transaction Authorization 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 may be requested online via Connect when you are conducting specific financial transaction. Each TAC is valid for a single transaction only and will expire after three (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 authorized officer of HLBCAM.

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 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 Connect website, HLBCAM 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 Connect when there is no activity detected for a period of time.
- Disallow access of 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 HLBCAM, 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 Connect or the mobile phone you use to receive your TAC or such other security codes, which HLBCAM 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.
- Do not click on internet links provided in email/SMS which directs you to a Hong Leong Bank (Cambodia) PLC Connect website. Always manually type our URL address. www.hongleongconnect.com.kh in your internet browser.
- Always ensure that you are on a genuine Connect website by checking the secure protocol on current domain (https://) and SSL certificate (represented by a lock/key sign) besides the green address bar on your browser.
- 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.