REVISION OF HSBC BANK TERMS & CONDITIONS FOR PERSONAL INTERNET BANKING

8 May 2019

Dear Valued Customers,

We will be introducing a simplified log-on journey to the new HSBC Malaysia Mobile Banking App with the choice of using biometric credentials (Face ID / Touch ID/Finger ID) or a 6-Digit PIN. The launch date of this simplified log on journey is to be announced soon.

In view of the upcoming changes, please be informed that HSBC Bank Terms & Conditions for Personal Internet Banking (October 2018 Edition) has been revised and the amended terms and conditions will come into effect on 29 May 2019 for all new and existing customers of HSBC Bank.

Updates include:-

1. Clauses 1, 2 and 3 will be revised as follows in relation to the provision of and access to Mobile Banking application:

1. **Services**
   a. HSBC Bank Malaysia Berhad (the 'Bank' which shall, include its successors and assigns) shall provide online services and facilities from time to time (the 'Services') through any Internet site established, operated and/or maintained by or on behalf of the Bank ('Internet Site') or on any mobile banking application (as updated from time to time) ('Mobile Banking App') to enable customers (each a 'Customer') to give instructions to and communicate with the Bank for the purposes of conducting banking, investment, financial and other transactions of various nature and obtaining services, products, information, goods, benefits and privileges from the Bank and where relevant, any members of the HSBC Group or any person as the Bank may consider necessary (the 'third party' which shall, include a third party service provider).
   b. As part of the Services, the Bank may make available via any Internet Site or Mobile Banking App, financial, market or other information and data ('Information') supplied by any person (each an 'Information Provider' which shall include any person who supplies any information to an Information Provider) and may provide reports compiled from Information in any form, medium or means ('Reports').
   c. The Bank has the right to determine and vary from time to time the scope and type of the Services to be made available in the Internet Site and the Mobile Banking App including, without limitation:
      i. expanding, modifying or reducing the Services at any time;
      ii. imposing and varying any restrictions on the use of the Services such as minimum and maximum daily limits with respect to the value of any transaction or any type of transactions which the Customer may conduct by using the Services;
      iii. Prescribing and changing the normal service hours during which the Services are available and any daily cut-off time for any type of Services or transactions. Any instruction of the Customer received by the Bank after any applicable daily cut-off time shall be deemed to be received on the next business day. The Bank may specify business day and daily cut-off time by reference to the time of various markets operating in different time-zones;
      iv. Reducing or re-setting a transfer limit (whether designated by the Customer or the Bank) to a lower value or down to zero if the Customer has not utilized the relevant Service(s) for a period of time that the Bank may designate from time to time;
      v. Prescribing the operating systems supported by the Bank from which the Customer can access the Services at the Internet Site and Mobile Banking App; and

HSBC

vi. Issuing new updates to the Internet Site and Mobile Banking App.

d. The Bank may require the Customer to nominate or register specific account(s) for the purposes of the Services.

e. Products and services referred to in the Internet Site and Mobile Banking App are offered only in Malaysia where they may be lawfully offered by the Bank or another member of the HSBC Group.

f. The Internet Site and the Mobile Banking App are to be accessed and used by the Bank's customers, and they are not intended for use or download by any person who is not already the Bank's customer or in any jurisdiction where such download or use would be contrary to any law or regulation of such jurisdiction or where the Bank is not licensed or authorised to provide the Services.

2. **Governing Terms and Conditions & Internet Banking Records**

a. The Services provide an additional means for the Customer to operate accounts, conduct transactions and obtain services, products, information, goods, benefits and privileges from the Bank and/or other members of the HSBC Group as shall be made available from time to time. Transactions effected by using the Services are subject to these terms and conditions and other related terms issued by the Bank including the Disclaimer, Internet Privacy Statement; Client Charter; Privacy and Security; Terms of Use and Hyperlink Policy currently published on the Internet Site and Mobile Banking App of the Bank where the Services are provided and the User Guide (collectively, 'Terms and Conditions'). All other terms and conditions governing the relevant accounts, transactions, dealings, services, products, information, goods, benefits or privileges shall continue to apply but where there is any discrepancy, this Terms and Conditions shall prevail for the purposes of the Services.

b. Where the Customer gives an Instruction (as defined below) or requests a transaction through the Services:

- The Terms and Conditions will apply in addition to the existing terms and conditions in respect of the Customer's dealings with the Bank in respect of particular accounts or products or generally even if the Customer have not signed such terms and conditions, including without limitation, the Bank's Universal Terms and Conditions (consisting of the Bank's Generic Terms and Conditions, Specific Terms and Conditions for HSBC Premier and HSBC Advance, Specific Terms and Conditions for Retail Banking and Wealth Management and Cardholder Agreement) as amended from time to time. In the event of any inconsistency, this Terms and Conditions will prevail for the purposes of the Services; and
- The Customer hereby undertakes to observe and comply with all applicable laws of Malaysia and the regulations, notices and directives issued by Bank Negara Malaysia (in particular, the BNM Notices on Foreign Exchange Administration Rules) and any relevant authority.

c. The Bank's records, unless shown to be wrong, will be evidence of the Customer's dealings with the Bank in connection with the Services.

d. The Customer agrees not to object to the admission of the Bank's records as evidence in any legal proceedings because such records are not originals, are not in writing or are documents produced by a computer or electronic device.

3. **Use of the Services**

a. To subscribe for the Services, the Customer is required to maintain a Current or Savings Account with the Bank or be a holder of one or more cards, including without limitation, an Debit Card, credit, charge, or stored value card issued by the Bank ('Cards'). Not all accounts may be accessed under the Services and not all types of Cards may be used to register for the Services. For instance, if the Customer maintains a joint account, the Customer can sign up for the Services only if the mandate for the account allows the Customer to operate the account jointly and severally (such joint accounts shall be referred to as 'the eligible joint accounts' in this Clause). For details of accounts in respect of which the Services are currently available, please refer to the guidance and information set out on screen in the 'Help' pages of the Services and all other customer guides and other guidance issued by the Bank in connection with the Services, as amended from time to time ('User Guide').

b. The Customer's application for the Services is subject to the Bank's approval and where the Customer's application is rejected, the Bank is not obliged to provide any reason(s) therefore.

HSBC

c. To access the Services for the first time via Internet Site, the Customer is required to register online at www.hsbc.com.my and to access the Services via Mobile Banking App, the Customer is required to download and install the Mobile Banking App from the official supplying application store on their electronic devices or in such other manner as the Bank may from time to time specify and indicate his acceptance of all the terms and conditions governing the use of the Services and to provide such information as the Bank may reasonably specify for identifying him.

d. By registering to use the Services, the Customer warrants that all information provided by the Customer to the Bank in relation to the Services is true, complete and up-to-date.

e. The Services are for the sole and exclusive use by the Customer.

f. The Customer shall not use or knowingly allow any other person to use the Services, the Information and/or the Reports for or in connection with any illegal purpose or activity; or any business or commercial purpose or activity. The Customer shall notify the Bank as soon as practicable if he becomes aware of such use.

g. Any exchange rate, profit rate, dealing rate and other prices and information quoted by the Bank on the Internet Site or Mobile Banking App or otherwise in response to an online inquiry is for reference only and is not binding on the Bank. Any rate, price and information offered by the Bank for the purpose of the relevant transaction shall be binding on the Customer upon the Customer confirming his acceptance irrespective of any different rate, price or information quoted by the Bank.

h. The Customer acknowledges that there may be a time lag in transmission of instructions, information or communication via the Internet.

i. For Mobile Banking App, updates will be downloaded automatically for some devices. If this does not happen, the Customer shall download the update from the supplying app store. The Customer should log on to the Mobile Banking App regularly to check any in-App messages displayed by the Bank which may include reminders to the Customer to install new updates. The Customer acknowledges that the Customer may not be able to use the Mobile Banking app until the latest updated version has been downloaded and installed.

j. Certain Services made available through the Internet Site and/or Mobile Banking App may require information about the Customer's physical location sent from the Customer's computer or electronic device (for example, Find a Branch/ATM requires usage of GPS signals). If the Customer uses such Service, the Customer consents to the Bank, its partners, licensees, and Google or any other approved third party service providers accessing, monitoring, transmitting, collecting, maintaining, disclosing, processing and using the Customer's location data to enable the Bank and Google or any other approved third party service providers to provide the relevant functionality in accordance with the terms and conditions, and privacy policy, of the Bank and those of Google or any other approved third party service providers. The Customer will be asked to consent to the use of location services the first time the Customer uses the relevant Services. The Customer may withdraw consent at any time by turning off the location services settings on the computer or electronic device.

k. Access to third party services (such as Google Maps/Google Earth API) through the Mobile Banking App is subject to separate terms and conditions of third party service providers (such as Google terms and conditions available at http://maps.google.com/help/terms_maps.html and http://www.google.com/enterprise/earthmaps/legal/universal_aup.html).

2. Clause 4 will be revised as follows in relation to biometric credentials and 6-DigitPIN:

a. Definitions

- "Security Device" means the electronic device which generates the Security Code, Re-authentication Code and Transaction Signing Code.
- "Security Device PIN" means the personal identification number adopted by the Customer for using the Security Device and includes any replacement number.
- "6-Digit PIN" means the personal identification number adopted by the Customer for logging on to the Mobile Banking App on customer's own mobile devices registered with the Bank.
- "Security Code" means the one-time numeric password generated by the Security Device for access to the Services.
- "Re-authentication Code" means the one-time numeric password generated by the Security Device for performing selected transactions.

- "Transaction Signing Code" means the one-time numeric password generated by the Security Device for performing selected transactions after the relevant numeric password relating to each transaction is keyed-in into the Security Device.
- The Security Code, the Re-authentication Code and the Transaction Signing Code shall collectively be referred to as the Security Device Codes.
- "Biometric Credentials" means any unique biological characteristics or traits that verify the identity of a person, such as fingerprints, eye retinas, face and voice recognition.

b. The Customer shall follow the guidance provided by the Bank online in designating the user identification code (the 'User ID'), the password (the 'Password'), the secondary password (the 'Secondary Password') , SMS Code , Security Device PIN , 6-Digit PIN, Security Code, and Security Device Codes and Biometric Credentials for identifying the Customer for the purposes of the Services and for performing transactions in respect of the Services.

c. The Customer may change the Password, the Secondary Password, and the Security Device PIN and 6-Digit PIN at any time but any change shall be effective only if accepted by the Bank.

d. The Bank shall may require the Customer to use the Security Device Codes to access and use any of the Services. It is the sole responsibility of the Customer to apply to the Bank for a Security Device or a replacement if a Security Device has previously been issued but is subsequently lost or has failed to function as intended.

e. Notwithstanding Clause 4(c) above, the Customer may perform selected transactions, as determined by the Bank, in the absence of a Security Device when they have designated and possess their User ID, Password, Secondary Password , SMS Code, 6 Digit PIN and/or Biometric Credentials.

f. The Customer shall act in good faith, exercise reasonable care and diligence in keeping the User ID, the Password, the Secondary Password, the Security Device PIN, the 6-Digit PIN, the Security Device Codes and the SMS Code in secrecy. For example, the Customer should not:

- Write or otherwise record the User ID, Password, Secondary Password, and Security Device PIN and 6-Digit PIN in a way that can be understood by someone else;
- Share the Password, the Secondary Password, and the Security Device PIN and the 6-Digit PIN with someone else including, without limitation, the Bank's employees and any third parties providing account aggregation services;
- Destroy any advice from the Bank concerning the Customer's PIN, namely the Customer's Card Personal Identification Number; or the Personal Identification Number issued to the Customer with the Customer's User ID when the Customer first applied for the Bank's Telebanking services, promptly after receipt;
- Use Passwords, Secondary Passwords, and Security Device PINs and 6-Digit PINs which may be easy to guess such as birthdays, telephone numbers, dates of birth etc.;
- Record his/her User ID, Password, Secondary Password, or Security Device PIN or 6-Digit PIN on any software which retains it automatically (for example, any computer screen prompts or 'save password' feature or the like on an internet browser);
- Use the same Password, Secondary Password, and Security Device PIN and 6-Digit PIN without regularly changing it;
- Use Passwords, and Secondary Passwords, Security Device PIN and the 6-Digit PIN from other internet sites or mobile applications;
- At no time and under no circumstances shall the Customer disclose the User ID, the Password, the Secondary Password, the Security Device PIN, the 6-Digit PIN, the Security Device Codes and/or SMS Code to any other person or permit the Security Device to come into the possession or control of any other person.

g. The Customer shall be fully responsible for any accidental or unauthorized disclosure of the User ID, the Password, the Secondary Password, the Security Device PIN, the 6-Digit PIN, the Security Device Codes and/or SMS Code to any other person and shall bear the risks of the User ID, the Password, the Secondary Password, the Security Device PIN, the 6-Digit PIN, the Security Device Codes or SMS Code, Biometrics Credentials and electronic devices being used by unauthorized persons or for unauthorized purposes.

h. Upon notice or suspicion of the User ID, the Password, the Secondary Password, the Security Device PIN, the 6-Digit PIN, the Security Device Codes and/or SMS Code being disclosed to, and/or the Security Device and/or electronic devices in which the Mobile Banking App was installed on being lost or has otherwise come into the possession or control of any unauthorized person or any unauthorized use of the Services being made, the Customer shall notify the Bank in person as soon as practicable or by telephone at such telephone number(s) as the Bank may from time to time prescribe (and the Bank may ask the Customer to confirm in writing any details given) and, until the Bank's actual receipt of such notification, the Customer shall remain responsible for any and all use of the Services by unauthorized persons or for unauthorized purposes.

i. If the Customer allows usage of his/her Biometric Credentials in using some of the Services, the Customer shall ensure that the Customer's Biometric Credentials stored on device are the Customer's own and do not store anyone else's Biometric Credentials on the Customer's device and that the Customer only use his/her own Biometric Credentials to log on to the Mobile Banking App. The Customer must take all reasonable precautions to keep safe and prevent fraudulent use of Biometric Credentials stored on the Customer's device.

j. The Customer should not use facial recognition for authentication purpose in the following situations:-

- The Customer has an identical twin sibling, or
- The Customer is an adolescent where facial features may be undergoing a rapid stage of development.

3. Clause 7 will be revised as follows in relation to the use of Mobile Banking App:

a. The Customer shall provide such information as the Bank may from time to time reasonably request for the purposes of providing the Services. The Customer shall also ensure that all information provided to the Bank is at all times accurate, complete and up-to-date including, without limitation, the Customer's address and other contact details.

b. The Customer understands that the Bank needs to and so authorizes the Bank to use, disclose, compile, match, obtain and/or exchange, process, share, store or transmit information about the Customer, the Customer's account(s), affairs, facilities which the Customer may have with the Bank and/or the transaction(s) ("Customer's Information") executed by the Bank on the Customer's behalf to, from or with any person in any jurisdiction (including Malaysia), including, without limitation,

   i. Any bureaus or agencies established or to be established by Bank Negara Malaysia ('BNM') which includes, without limitation, the Central Credit Bureau who will store the Customer's Information in the Central Credit Reference Information System ('CCRIS') or the Association of Banks Malaysia ('ABM') or by other government or regulatory authority;
   ii. Any member of the HSBC Group; and
   iii. Any third party including any debt collection agencies that may be appointed by the Bank.
   iv. The Bank undertakes that any such usage, disclosure, compilation, matching, processing, sharing, storage or transmission of information will be done on a confidential basis and the Bank will endeavour to maintain the strict confidentiality of such information within the HSBC Group unless (a) otherwise required or permitted by any applicable law, regulation or request of any public or regulatory authority; or (b) disclosure is required for the purposes of preventing fraud; or (c) the Bank deems disclosure necessary to provide the Services.

c. The Customer shall not, and shall not attempt to decompile, reverse-engineer, translate, convert, adapt, alter, modify, enhance, add to, delete or in any way tamper with, or gain access to, any part of the Services or any Internet Site or any Mobile Banking App or any software comprised in them.

d. The Customer acknowledges that it is the responsibility of the Customer to determine independently market prices and rates for trading purposes through his usual trading channels, to verify any Information and/or Report before relying or acting on it and to seek independent professional advice on legal, tax and other issues in connection with the use of the Services, the Information and the Reports, the Terms and Conditions and any transactions and dealings which may affect the Customer under all applicable laws.

e. The Customer agrees to comply with the Terms and Conditions and any security measures and procedures mentioned in them.

f. Once the Customer has logged on to the Services, the Customer must not leave the Internet Site or Mobile Banking App from which the Customer has accessed the Services at any time; or let anyone else use the Internet Site or Mobile Banking App until the Customer has logged off the Services. The Customer will be responsible for ensuring that he/she has logged off the Services at the end of any session.

g. The Customer must not access the Services from any computer or electronic device connected to a local area network (LAN) or any public internet access device or access point without first making sure that no-one else will be able to observe or copy the Customer's access or get access to the Services pretending to be the Customer.

h. The Customer must inform the Bank immediately of any unauthorized access to the Services or any unauthorized transaction or instruction which the Customer knows of or suspects or if the Customer suspects someone else knows his/her Password and/or Secondary Password. The Customer may do so in person or at such telephone number (s) the Bank may prescribe from time to time. The Bank may ask the Customer to confirm in writing the details given. The Customer must also change his/her Password and/or Secondary Password immediately to a number/string of characters which the Customer has not used before. The Bank will need the Customer to help the Bank and the police in trying to recover any losses. The Bank may disclose information about the Customer or the Customer's account to the police or other third parties if the Bank thinks it will help prevent or recover losses.

i. The Customer agrees to check carefully his/her records of transactions and statements of accounts and inform the Bank immediately (at any rate, within 60 days of receipt by the Customer of such records and/or statement) of any discrepancy, failing which the Bank shall accept no responsibility whatsoever for such discrepancy.

j. Customers should install personal firewall and anti-virus software onto their computer(s) and electronic device(s) (and have them updated regularly) and only conduct transactions online if they are satisfied that the website or mobile application is valid, secure and reputable. The Customer hereby irrevocably and unconditionally agree that, further to Clause 9 herein, the Bank will not be liable for any losses, damage or injury that the Customer may suffer where it is determined that the Customer has failed to take the aforesaid precautionary steps resulting in him/her incurring such losses, damage or injury.

k. The Customer must not use the Mobile Banking App on any device or operating system that has been modified outside the mobile device or operating system vendor supported or warranted configurations. This includes devices that have been "jail-broken" or "rooted". A jail broken or rooted device means one that has been freed from the limitations imposed on it by your mobile service provider and the phone manufacturer without their approval. The use of Mobile Banking App on a jail broken or rooted device may compromise security and lead to fraudulent transactions. Download and use of the Mobile Banking App in a jail broken or rooted device is entirely at the Customer's own risk and the Bank will not be liable for any losses or any other consequences suffered or incurred by the Customer as a result.

l. The Customer is responsible for any ancillary cost when accessing the Services at the Internet Sites and Mobile Banking App, such as charges by the Customer's network operator for downloading and/or accessing the Internet Site and Mobile Banking App including updates to the Mobile Banking App.

m. The Customer is responsible to delete the Mobile Banking App from his/her device if the Customer changes device or dispose of it.

4. New Clause 9(g) will be added as follows:

   g. The Bank and any member of the HSBC Group will not be liable for any failure to provide Services, in part or in full, due to abnormal and unforeseen circumstances beyond the Bank's control, the consequences of which would have been unavoidable despite all efforts to the contrary. This includes but not limited to, any phone or Internet network failures, for example, the Customer is not in an area of mobile network coverage.

5. Clause 18(a) will be revised as follows:

   a. The Services and the Terms and Conditions shall be governed by and construed in accordance with the laws of Malaysia. The Customer must comply with all applicable laws and regulations that govern the usage of the Services.

6. A new definition on 'Beneficiary of Fraud' will be added in Clause 19 as follows:

HSBC

Beneficiary of Fraud	means party who ultimately benefits from an Unauthorized Payment Instruction, or Fraudulent Payment Instruction.

The revised HSBC Bank Terms & Conditions for Personal Internet Banking (May 2019 Edition) is available here.