BOCHK Brunei Branch Mobile Token FAQ

1. **What is "Mobile Token"?**
   ★ "Mobile Token" is a feature of BOCHK Brunei Branch Mobile App. Upon activation of "Mobile Token" with a designated mobile device ("mobile phone"), you can use it immediately and authenticate transactions without bringing along with your "Security Device". Besides, "Mobile Token" supports passcode and Biometric Authentication usage, giving you a simple and convenient experience.

2. **Are there any charges for "Mobile Token"?**
   ★ It is free of charge for "Mobile Token".

3. **When do I need to use "Mobile Token"?**
   ★ You can use "Mobile Token" to generate one-time "Security Code"/ "Transaction Confirmation Code" to confirm designated transactions on Internet Banking or Mobile Banking.

4. **How do I activate "Mobile Token"?**
   ★ In order to activate "Mobile Token", you need to have a personal Internet Banking account, activate auto-lock function and install the latest version of BOCHK Brunei Branch Mobile App on your mobile phone and register a valid mobile number with the Bank.
   ★ Step 1: Click "Mobile Token > Activate" on homepage or "Menu > Settings > Mobile Token Setting> Activate Mobile Token > Activate"
   ★ Step 2: To register Biometric Authentication (you should enable the biometric recognition function on your mobile phone), click "Agree & Register Fingerprint / Face ID" and verify your biometric credential on the mobile phone; or click "Later" to go to Step 3
   ★ Step 3: Set up "Mobile Token" passcode
   ★ Step 4: Enter the One Time Password (OTP) sent by the Bank via SMS and click "Confirm" to complete the activation

5. **How can I generate one-time "Security Code" or "Transaction Confirmation Code" by using "Mobile Token"?**

- ★ For conducting designated transactions on Mobile Banking, "Mobile Token" will be used automatically, please follow the instructions to complete the transaction.
- ★ For conducting designated transactions on Internet Banking, please follow the instructions on Internet Banking to choose the required one-time Security Code type. Enter the specific transaction information (if required) and use Biometric Authentication or "Mobile Token" passcode to confirm. The Security Code will be generated, please enter the code to confirm the transaction.

6. **Can I activate "Mobile Token" on different mobile phone?**
   - ★ You can only activate "Mobile Token" on one mobile phone.

7. **If I forget to bring my mobile phone, can I activate "Mobile Token" on others' mobile phone?**
   - ★ For security reason, please do not login Mobile Banking and activate "Mobile Token" on others' mobile phone.

8. **If I changed a mobile phone, how can I transfer my "Mobile Token" to the new mobile phone?**
   - ★ You are required to download BOCHK Brunei Branch Mobile App on your new mobile phone and choose "Reset Mobile Token".

9. **Can I use "Mobile Token" and "Security Device" at the same time?**
   - ★ You can only use either "Mobile Token" or "Security Device". Upon successful activation of "Mobile Token", your "Security Device" will be suspended immediately. Please keep your "Security Device" properly. If necessary, you can reactivate your "Security Device" on Internet Banking within one year upon suspension of "Security Device".

10. **How can I reactivate my "Security Device"?**
    - ★ You can reactivate your "Security Device" through **"Setting > Security Setting > Reactivate the Security Device"** in Internet Banking after suspension of "Mobile Token".

11. What should I do if my "Mobile Token" was locked owing to repeatedly inputting invalid one-time Security Code / Transaction Confirmation Code on Internet Banking, or invalid "Mobile Token" passcode on Mobile Banking?
   - ★ You can click **"Menu > Settings > Mobile Token Setting > Reset Mobile Token"** in Mobile Banking and follow the instructions to reset your "Mobile Token".

12. What should I do if I forget my "Mobile Token" passcode?
   - ★ You can click **"Menu > Settings > Mobile Token Setting > Reset Mobile Token"** in Mobile Banking and follow the instructions to reset your "Mobile Token".

13. How can I change my "Mobile Token" passcode?
   - ★ You can click **"Menu > Settings > Mobile Token Setting > Reset Mobile Token"** in Mobile Banking to reset your "Mobile Token" passcode.

14. How to enable or disable using Biometric Authentication to login Mobile Banking and generate Security Code?
   - ★ You can enable or disable the setting through **"Menu > Settings > Mobile Token Setting > Enable Biometric Authentication Login and Use Mobile Token"** in Mobile Banking.

15. How to suspend my "Mobile Token"?
   - ★ You can suspend "Mobile Token" through the following ways:
   - ★ Click **"Menu > Settings > Mobile Token Setting > Suspend Mobile Token"** in Mobile Banking and follow the instructions to suspend your "Mobile Token".
   - ★ If your mobile phone is lost or stolen, you may contact Customer Service Hotline (673) 245 9858 or visit our branch.

16. What should I do if my mobile phone with activated "Mobile Token" is lost or stolen?
   - ★ You may use another mobile phone to log into Mobile Banking with your Internet Banking No. /User Name and password, click **"Menu > Settings > Mobile Token Setting > Suspend Mobile Token"** and follow the instructions to suspend "Mobile Token".

★ Please contact our Customer Service Hotline (673) 245 9858 or visit our branch to suspend "Mobile Token".

17. Do I need any network connection on my mobile phone to use "Mobile Token"?

★ When you are activating "Mobile Token", the network connection is required. After activation, you can still generate one-time Security Code or Transaction Confirmation Code while without network connection. For security reasons, you need to resume network connection to continue using "Mobile Token" when it is used for a specified number of counts or period of time defined by the Bank.

18. Which mobile phones are eligible for "Mobile Token"?
- ★ You can activate "Mobile Token" on mobile phones:
- ★ iPhone 5s or higher model with iOS 10.0 or above
- ★ Samsung, Huawei, Xiaomi, LG, Sony, Google, Nokia, Asus, Oppo*, HTC and Vivo mobile phones with Android 6.0 or above

* Only applicable to the below Oppo devices:
- ★ A93s 5G Mainland Version(PFGM00)
- ★ Reno6 5G Mainland Version (PEQM00)
- ★ Reno6 Pro 5G Mainland Version (PEPM00)
- ★ Reno6 Pro+ 5G Mainland Version (PENM00)
- ★ Reno5 5G Mainland Version (PEGM00)
- ★ Reno5 Pro 5G Mainland Version (PDSM00)
- ★ Reno5 Pro+ 5G Mainland Version (PDRM00)
- ★ A95 5G Mainland Version (PELM00)
- ★ K9 5G Mainland Version (PEXM00)
- ★ Find X3 Mainland Version (PEDM00)
- ★ Find X3 Pro Mainland Version (PEEM00)
- ★ A53 5G Mainland Version (PECM30)
- ★ Reno 4 SE 5G Mainland Version (PEAM00)
- ★ K7x Mainland Version (PERM00)
- ★ Reno 4 5G Mainland Version (PDPM00)
- ★ Reno 4 Pro 5G Mainland Version (PDNM00)
- ★ Reno 3 5G Mainland Version (PDCM00)
- ★ Reno 3 Pro 5G Mainland Version (PCRM00)

- ★   A91 Mainland Version (PCPM00)
- ★   Reno 10X Zoom Overseas Version (CPH1919)
- ★   Reno 10X Zoom Overseas Version (CPH1919)
- ★   Reno Z Overseas Version (CPH1979)
- ★   F11 Overseas Version (CPH1911)
- ★   Reno 10X Mainland Version (PCCM00)
- ★   Reno 2 Mainland Version (PCKM00)
- ★   Reno Mainland Version (PCAM00)
- ★   A11x Mainland Version (PCHM30)
- ★   A9 Mainland Version (PCAM10)

Biometric Authentication

i. Fingerprint Authentication

1. **If I fail to login using "Fingerprint Authentication" for multiple times, will my Mobile Banking be suspended?**
   - ★   Your Mobile Banking will not be suspended. However, your mobile phone may be locked, depending on the model of your mobile phone.

2. **Is my fingerprint stored in BOCHK?**
   - ★   The "Fingerprint Authentication" is performed by interfacing with the fingerprint authentication module of the mobile phone. The Bank does not store your fingerprint. Please note that if you have registered "Fingerprint Authentication", after disabling "Fingerprint Authentication" or suspending "Mobile Token", your fingerprint will be continuously stored on your mobile phone. You may consider cancelling the data at your decision. Please refer to the Terms and Conditions for use of Biometric Authentication for Mobile Banking.

3. **I have multiple fingerprints registered on my mobile phone. Can all of them be used to login Mobile Banking and use "Mobile Token"?**

- ★ When you register "Fingerprint Authentication", any fingerprints stored on your mobile phone can be used to login Mobile Banking and use "Mobile Token". Please ensure that only your fingerprints are stored on your mobile phone, and ensure the security of the security passcode that you can use to register your fingerprints on the mobile phone. For security reasons, do not register fingerprint(s) of other person(s) on your mobile phone or use jailbroken or rooted mobile phone. Please refer to the relevant Terms and Conditions and Security Information of our website for details.

4. **If I change fingerprint record(s) on my mobile phone, can I use "Fingerprint Authentication"?**
   - ★ If you change the fingerprint records(s) (e.g. add and/or delete fingerprint) on your mobile phone, you are required to login Mobile Banking with Internet Banking No. /User Name and password, and reset "Mobile Token".

5. **Why did my "Fingerprint Authentication" become invalid?**
   - ★ Your "Fingerprint Authentication" may become invalid for any one of the following reasons:
   - ★ Your Internet Banking account was cancelled or temporary suspended owing to input incorrect password continuously;
   - ★ You have activated "Mobile Token" on another mobile phone; ★ Your fingerprint information have changed; or already disabled "Fingerprint Authentication" or "Mobile Token".

6. **How many fingerprint(s) I can register to login Mobile Banking and use "Mobile Token"?**
   - ★ It depends on the number of fingerprint(s) that can be stored on your mobile phone. For security reasons, do not register fingerprint(s) of other person(s) on your mobile phone or use jailbroken or rooted mobile phone. Please refer to the relevant Terms and Conditions and Security Information of our website for details.

ii. Face ID Authentication

1. **If I fail to login using "Face ID Authentication" for multiple times, will my Mobile Banking be suspended?**
   - ★ Your Mobile Banking will not be suspended. However, your mobile phone may be locked, depending on the models of your mobile phone.

2. **Is my facial map stored in BOCHK?**
   - ★ The "Face ID Authentication" is performed by interfacing with the Face ID authentication module of the mobile phone. The Bank does not store your facial map. Please note that if you have registered "Face ID Authentication", after disabling "Face ID Authentication" or suspending "Mobile Token", your facial map will be continuously stored on your mobile phone. You may consider cancelling the data at your decision. Please refer to the Terms and Conditions for use of Biometric Authentication for Mobile Banking.

3. **If I change the facial map record on my mobile phone, can I use "Face ID Authentication"?**
   - ★ If you change the facial map record on your mobile phone, you are required to login Mobile Banking with Internet Banking No. /User Name and password, and reset "Mobile Token".

4. **Why did my "Face ID Authentication" become invalid?**
   - ★ Your "Face ID Authentication" may become invalid for any one of the following reasons:
   - ★ Your Internet Banking account was cancelled or temporary suspended owing to input incorrect password continuously;
   - ★ You have activated "Mobile Token" on another mobile phone;
   - ★ Your facial map record have changed; or already disabled "Face ID Authentication" or "Mobile Token".

5. **Should I enable "Face ID Authentication" if my siblings and I look alike or I am an adolescent?**

- ★ You must not use Biometric Authentication if you have reasonable belief that other people may share identical or very similar biometric credential(s) of you or your biometric credential(s) can be easily compromised. For instance, you must not use facial recognition for authentication purpose if you have identical twin or triplet sibling(s).
- ★ You must not use Biometric Authentication if the relevant biometric credential(s) of you are or will be undergoing rapid development or change. For instance, you must not use facial recognition for authentication purpose if you are an adolescent with facial features undergoing rapid development.