"Terms and Conditions for Digital Token Service"

Before using the Mobile Banking application ("Mobile Banking") of Industrial and Commercial Bank of China Singapore (referred to as "the Bank" or "our bank"), customers should carefully read these terms and conditions ("Terms and Conditions") for the Digital Token service.

The "Digital Token" service is part of the Mobile Banking service. These Terms and Conditions are additional to the "Mobile Banking Terms and Conditions" published on our bank's website (singapore.icbc.com.cn). Customers should refer to both sets of terms and conditions, and in case of any conflict, these Terms and Conditions shall prevail.

**I. Definitions and Interpretations**

1."Digital Token" refers to the dedicated electronic version security encryption function provided by the Bank specifically for Mobile Banking, which has an equivalent security level to the current "Physical Token." It is a non-physical medium and serves as a method for dual authentication of designated transactions in Mobile Banking.

2."ICBC SG Mobile Banking" or "Mobile Banking" refers to the mobile application developed by the Bank specifically for iOS and Android mobile platforms.

1. "Physical Token" refers to the transaction authentication device issued by the Bank, bundled with the customer's Mobile Banking, when opening an account and activating Mobile Banking. It is a physically existing electronic authentication tool.

4."Mobile SMS Dynamic Password" refers to the one-time verification code sent by the Bank to the customer's registered mobile number at the time of account opening. It is used as a dual authentication method to verify the customer's identity during designated transactions in Mobile Banking.

5."Authorized mobile device" refers to the device agreed upon by the customer for using the electronic security encryption function of Mobile Banking.

6."Biometric authentication" refers to the functionality that identifies the customer's identity using fingerprint, facial recognition, or other biometric features.

**II. Important Statements**

7.Customers must adhere to these Terms and Conditions when using the Digital Token. By opening and using the Digital Token, customers are deemed to have accepted and bound by these Terms and Conditions. If customers do not accept these Terms and Conditions, they should not open or use Digital Token.

8.The use of Digital Token in Mobile Banking is a verification method for confirming the customer's identity and ensuring transaction security. Customers can activate Digital Token on the authorized mobile device by completing the Bank's designated steps. After successful activation, customers can confirm their identity and complete related transaction verification by entering the Digital Token password on the authorized mobile device. For Mobile Banking customers who hold other designated authentication tools from the Bank ("Physical Token" or "Mobile SMS Dynamic Password"), they do not need to use the "Physical Token" after activating Digital Token. However, customers can still choose to use "Mobile SMS Dynamic Password" or other designated authentication tools specified by the Bank for secure authentication of designated transactions in Mobile Banking.

1. Customers can cancel Digital Token at any time through Mobile Banking following the Bank's designated steps. Once canceled, if customers still have other designated authentication tools from the Bank ("Physical Token" or "Mobile SMS Dynamic Password"), they can continue to use and complete secure authentication for designated transactions in Mobile Banking. However, if customers do not have any other designated authentication tools from the Bank, they will not be able to perform secure authentication for designated transactions in Mobile Banking.
2. Customers are only allowed to set up Digital Token on one authorized mobile device at a time, and the Bank will use the customer's mobile device as one of the identification elements. If customers store the biometric credentials of any other person on the authorized mobile device or allow the biometric credentials of any other person to be stored on the authorized mobile device, customers shall be responsible if anyone authenticates mobile banking logins and transactions with alternative biometric credentials. The Bank is not required to further inquire into the authorization, identity, or accuracy of such instructions or agreements made by individuals, even in the presence of errors, misunderstandings, fraud, impersonation, or lack of clear authorization. All such transactions and dealings will be deemed authorized by the customer and shall be binding on the customer.

Customers shall bear all risks and losses arising from the use of Biometric Authentication, and the Bank shall not be responsible for any losses or any other consequences incurred or suffered by the customers.

11. Customers must fully understand and agree that the Digital Token does not completely replace other security verification methods. Customers should take all reasonable security measures to prevent unauthorized use or fraudulent theft of the Digital Token, including but not limited to:

a. Customers should take reasonable precautions to safeguard their authorized mobile device, mobile banking username and password, and Digital Token password to prevent loss or fraudulent theft.

b. Customers shall not use mobile banking and Digital Token on authorized mobile devices or operating systems that are modified beyond the scope of support or warranty provided by the device or operating system provider. Such devices include those that have been jailbroken or rooted. "Jailbroken" or "rooted" devices refer to devices that have had their restrictions removed without the approval of the mobile service provider and phone manufacturer. Using mobile banking and Digital Token on "jailbroken" or "rooted" devices may compromise security features and lead to fraudulent transactions. Customers assume all risks associated with downloading and using mobile banking and Digital Token on "jailbroken" or "rooted" devices. The Bank shall not be responsible for any losses or other consequences incurred or suffered by the customer as a result.

c. If customers become aware of or suspect unauthorized use of their authorized mobile device or Digital Token password, they should promptly change the Digital Token password or cancel the mobile banking digital token or notify the Bank by calling the customer service hotline at (65) 63695588, if feasible.

d. If customers lose their authorized mobile device, they should reset the Digital Token functionality on another device to render the Digital Token functionality on the lost device ineffective.

12. The Bank reserves the right to specify, modify, suspend, or terminate the scope and features of the Digital Token from time to time without prior notice, as it deems necessary or appropriate.

1. The Bank reserves the right to revise the content of these Terms and Conditions from time to time.

14. Notices regarding revisions will be sent via the mobile banking app or the Bank's online portal. Any revisions made by the Bank to these Terms and Conditions shall take effect immediately upon notification and shall be binding on the customer.

**III. Applicable Law and Jurisdiction**

These Terms and Conditions are governed by and shall be construed in accordance with the laws of Singapore. Any disputes arising from these Terms and Conditions shall be subject to the jurisdiction of the courts of Singapore.

*(end of page)*