

October 2025

Notice of Enhanced Protection for Internet Banking Login and Amendments to the Related Terms and Conditions

Dear Valued Customers,

In order to further protect customers from digital frauds and scams, Nanyang Commercial Bank, Limited (the "Bank") will undergo a system update from 7:00 pm to 11:00 pm on 27 November 2025 (the "System Update") to **enhance protection for Internet Banking login**. Following the System Update, **the Bank's terms and conditions related to Internet Banking will be updated** accordingly. During the System Update, the Internet Banking services remain. The details are as follows:

I. Enhanced Protection for Internet Banking Login

Following the System Update, the Bank will enhance protection for Internet Banking login.

Currently, you are required to enter your Internet Banking No./Username, password, and verification code when logging on to Internet Banking. **After the System Update, if you have a Security Device or enabled Mobile Token, you must log on to Internet Banking with two-factor authentication.** Apart from Internet Banking No./Username, password, and verification code, you are further required to input the one-time security code generated by (1) Security Device or (2) Mobile Token prior to accessing Internet Banking.

For more information on Internet Banking Login with two-factor authentication, please refer to the enclosed Appendix 1.

II. Amendments to terms and conditions related to Internet Banking



Due to enhanced protection for Internet Banking login and amendments to other identity verification method, following the System Update, the Bank will amend the "Terms and Conditions and Important Statements for Personal Mobile Banking and Internet Banking Services", "Terms and Conditions for use of Biometric Authentication for Mobile Banking", "Terms and Conditions for Small Value Transfer Service" and "Binding Service Guide" accordingly, details of which are outlined in Appendix 2 to Appendix 5 of this Notice. You are advised to read the amendments before you continue to use the relevant services. Please note that you will be deemed to have agreed to the amendments if you continue to use the relevant services of the Bank after the System Update. The Bank may not be able to continue to provide the relevant services if you do not accept the amendments. You may also notify the Bank to discontinue the relevant services before the System Update.

You may download the current "Terms and Conditions and Important Statements for Personal Mobile Banking and Internet Banking Services", "Terms and Conditions for use of Biometric Authentication for Mobile Banking", "Terms and Conditions for Small Value Transfer Service" and "Binding Service Guide" from the Bank's website (the Bank's website > 'Personal Banking' > 'Other Services' > 'Conditions and Rules for Services and Other Information') before the System Update. Please note that only the revised version will be available after the System Update.

You may download this Notice from the Bank's website (the Bank's website > 'About Us' > 'Notice') on or before 31 December 2025 (afterwards, you may not be able to read or download this Notice).

In case of any discrepancy between the English and the Chinese versions of this Notice, the English version shall prevail.

We sincerely apologize for any inconvenience it may cause you.

If you have any enquiries, please contact our staff or call our Customer



Service Hotline (852) 2616 6628.

Nanyang Commercial Bank, Limited

Appendix 1: User Guide for Internet Banking Login

Appendix 2: Amendments to "Terms and Conditions and Important Statements for Personal Mobile Banking and Internet Banking Services"

Appendix 3: Amendments to "Terms and Conditions for use of Biometric Authentication for Mobile Banking"

Appendix 4: Amendments to "Terms and Conditions for Small Value Transfer Service"

Appendix 5: Amendments to "Binding Service Guide"

Appendix 1: User Guide for Internet Banking Login

- **Login via Security Device / Mobile Token**

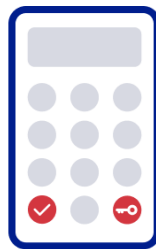
Step 1: By accessing to login page of Personal Internet Banking, enter your Internet Banking No./Username, password, and verification code. Then click "Login".

Step 2: Enter the one-time security code generated by (1) Security Device or (2) Mobile Token

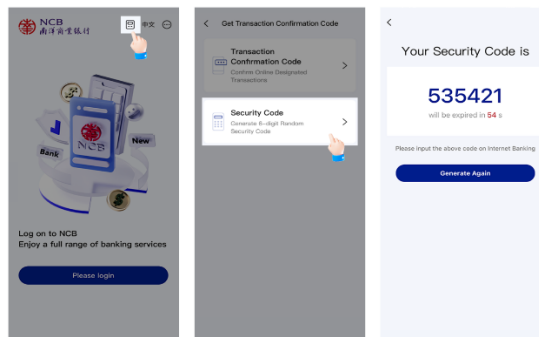
Step 3: Upon successful authentication, you may access to your Internet Banking

- **How to obtain the security code**

If you have enabled Security Device, you may press the button at the bottom right corner of the Security Device. A 6-digit security code will then be displayed.



If you have enabled Mobile Token, you may open the Personal Mobile Banking App (without proceeding login); click the "Mobile Token" at the upper right corner of the home page. By clicking "Security Code", a 6-digit security code will then be displayed.



Appendix 2: Amendments to “Terms and Conditions and Important Statements for Personal Mobile Banking and Internet Banking Services”

Clause	Details of Amendments (Revised contents are underlined and deleted contents are marked with strikethrough lines)
Access to Internet Banking and Personal Mobile Banking Services by using Security Token and Mobile Token	<p>1. Depending on the type of services you wish to access and/or use, you will be required to perform one or more of the following steps which the Company may in its sole discretion require <u>to access to Internet Banking and Personal Mobile Banking Services.</u> For details, please visit the "Security Information" on the official website of the Bank.</p> <p>i. Enter the correct combination of the Internet Banking Number / Login User Name / Mobile Phone Number and Login Password to log in to the Internet Banking Services;</p> <p>ii. Applying your biometric credentials registered under the specified model of mobile device for authentication purposes.</p> <p>4.If you disable the biometric credential authentication function of your Mobile Token, you can still use Mobile Token password to access your Mobile Token. If your biometric credential stored on your mobile device has been changed, your <u>biometric credential authentication function</u> Mobile Token will be suspended. You are then required to reactivate the Mobile Token function.</p> <p>7. You can apply for a new Security Token at any of our branches or use other authentication means as may be agreed by the Bank from time to time to conduct and authorize transaction instructions. However, upon successful activation of the Security Token, your Mobile Token will be cancelled automatically and you can no longer use biometric credential authentication for the Bank's Mobile Banking Services.</p>
The End User Terms of Using Online Identity Documents	<p><u>The End User Terms of Using Online Identity Documents Authentication</u> Use of “ZOLOZ Real ID Solution” in the Mobile Remote Account Opening Service</p>



<p>Authentication (originally known as Use of "ZOLOZ Real ID Solution" in the Mobile Remote Account Opening Service)</p>	<p>If you would like to make an application for <u>relevant services by using Online Identity Documents Authentication (e-KYC)</u> opening a bank account through our Bank's personal mobile banking services (the "Mobile Remote Account Opening"), you agree, to comply with the End User Terms of Use ("End User Terms") from Alibaba Cloud (Singapore) Private Limited ("Alibaba Cloud") and the third-party provider of the <u>Online Identity Documents Authentication (e-KYC) Solution e-KYC "ZOLOZ Real ID Solution"</u> (the "Solution"), in addition with other relevant terms and conditions. The End User Terms are as below (For the avoidance of doubt, "End User" shall refer to "you" as an individual end user):</p> <p>1. Usage - End User is permitted to access and use the Solution as incorporated into the Bank's Mobile Remote Account Opening, pursuant to the End User Terms, for the sole purpose of enabling End User to receive and/or use the <u>Bank's relevant services</u>. Bank's Mobile Remote Account Opening. End User shall not modify, reverse engineer, copy, sell, lease, or sublicense the Solution. End User may not extract ideas, algorithms, procedures, workflows or hierarchies from the Solution or otherwise use the Solution for the purpose of developing any other software based on concepts, functions, or operations similar to those in the Solution.</p> <p>7.Liability – TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, UNDER NO CIRCUMSTANCES SHALL THE BANK OR ALIBABA CLOUD BE LIABLE TO END USER FOR ANY DIRECT DAMAGES, LOSS OF PROFITS, REVENUE, DATA, REPUTATION OR GOODWILL, OR FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES FOR ANY MATTER RELATING TO THE SOLUTION, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE OR STRICT LIABILITY) OR OTHERWISE, AND EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. NOTWITHSTANDING THE FOREGOING, IF THE BANK OR ALIBABA CLOUD IS FOUND LIABLE DIRECTLY TO END USER FOR</p>
---	---

	<p>ANY DAMAGES, ITS TOTAL LIABILITY RELATED TO THESE END USER TERMS SHALL NOT EXCEED THE AMOUNT EQUAL TO THE LOWER OF (A) USD \$1,000,000.00 OR (B) THE FEES PAID BY END USER TO THE BANK FOR THE <u>RELEVANT MOBILE-REMOTE ACCOUNT-OPENING SERVICES</u> THAT INCORPORATES THE SOLUTION IN THE PRECEDING SIX (6) MONTHS PRIOR TO THE MONTH IN WHICH THE RELEVANT CLAIM IS FIRST MADE GIVING RISE TO LIABILITY. THE EXISTENCE OF MORE THAN ONE CLAIM OR CAUSE OF ACTION WILL NOT ENLARGE THE FOREGOING LIMIT.</p>
<p>Transaction Instructions</p>	<p>1. If you need to make any transaction instruction through the Internet Banking Services, you must use <u>the correct authentication information</u>, as notified by the Bank from time to time, the correct combination of the Internet Banking Number / Login User Name / Mobile Phone Number and Login Password / Biometric Credential Authentication and such other information as may be required by the Bank for the purposes of executing a transaction instruction through the Internet Banking Services. <u>For details, please visit the "Help Center" on the official website of the Bank.</u> Transaction instruction shall not be considered to be received by the Bank unless they are given in such manner as we may prescribe and has been actually received by the Bank.</p>
<p>Funds Transfer Services</p>	<p>3. In order to use the Funds Transfer Services, you <u>shall</u> must use a valid Security Code or otherwise authenticate the customer's identity through the usage of the Mobile Token. The Bank may require you to use Security Code or the Mobile Token in order to access any other Internet Banking Services.</p>

Appendix 3: Amendments to “Terms and Conditions for use of Biometric Authentication for Mobile Banking”

Clause	Details of Amendments (Revised contents are underlined and deleted contents are marked with strikethrough lines)
Terms and Conditions for use of biometric authentication for Mobile Banking	<p>2. You may use your biometric credential(s) (including without limitation fingerprint(s), facial map(s) or any other biometric data as approved by the Bank from time to time) stored on your designated mobile device to login the Bank's Mobile Banking, to authorize instruction in respect of transactions as specified by the Bank from time to time through the Bank's Mobile Banking or to do such other things or transactions as notified by the Bank from time to time. Designated mobile device means mobile devices with operating system version of iOS 12.0 or higher, Android 9.0 or higher and supporting biometric authentication function. The details may be accessed at the Bank's website "Help Center".</p>
	<p>5. The Conditions for Services may be accessed at <u>the Bank's website "The Conditions for Services"</u> https://www.ncb.com.hk/nanyang_bank/resource/tnc_en.pdf. In the event of any conflict or inconsistency, these Terms shall prevail over the Conditions for Services and to the extent of such conflict or inconsistency.</p>
	<p>6.</p> <p>iv. You must register the biometric authentication through the Bank's <u>designated means (The details may be accessed at the Bank's website "Help Center")</u> Mobile Banking by using your Internet Banking No./Username, password and SMS One-time password and choosing to use the relevant biometric credential(s) that you stored on your designated mobile device for the purpose of biometric authentication;</p> <p>ix. You may still choose to login Mobile Banking with Internet Banking No./Username and Password or authorize transaction instruction by using Security Code/Transaction</p>

	<p>Confirmation Code of Security Device or SMS One-time password or to conduct other transactions through the other authentication means as agreed by the Bank from time to time (<u>The details may be accessed at the Bank's website "Help Center"</u>).</p> <p>15 . The Bank reserves the right to amend, add or delete at any time these Terms by giving reasonable prior notice in writing to you and such notice may be made in such manner and by such means of communication as the Bank shall deem fit, including, without limitation, use of direct mailing material or advertisement, website display or electronic communications such as electronic mail. You acknowledge and agree that you shall observe and comply with any such amendment, addition and/or deletion when using the biometric authentication. Your continued use of the biometric authentication shall constitute your acceptance of any such changes or modifications.</p>
--	---

Appendix 4: Amendments to “Terms and Conditions for Small Value Transfer Service”

Clause	Details of Amendments (Revised contents are underlined and deleted contents are marked with strikethrough lines)
2.Set Up	<p>2.1 The customer must log on to the Mobile Banking or the Internet Banking and use the <u>authentication</u> SMS one-time verification code or any other means approved by the Bank for the registration of this service. Upon registration, any eligible bank account of the customer for the fund transfer can be used for this service. <u>For details, please visit the "Help Center" on the official website of the Bank.</u></p>

Appendix 5: Amendments to “Binding Service Guide” (Available in Chinese version only)

Clause	Details of Amendments (Revised contents are underlined and deleted contents are marked with strikethrough lines)
綁定服務指南	<p>1 (iii.) 進行綁定時請輸入以下資料：(a)個人網上銀行號碼 (b)個人網上銀行密碼及 (c)本行認可的驗證方式短訊<u>一次性驗證碼</u>。<u>有關詳情，請瀏覽本行官網“幫助中心”。</u></p> <p>3. 如用戶於網上銀行、手機銀行或微信累計連續 4 次錯誤輸入個人網上銀行密碼，用戶其名下的個人網上銀行密碼將被凍結並無法登入網上銀行。用戶可親臨本行各分行或透過個人網上銀行服務、個人手機銀行服務密碼重置功能辦理，釋放被凍結的密碼。<u>有關詳情，請瀏覽本行官網“幫助中心”。</u></p>