大新銀行
DAH SING BANK

有關 328 營商理財保安認證服務之條款及細則的修訂通知

由 2026 年 1 月 25 日（「生效日」）起，328 營商理財保安認證服務之條款及細則將被修訂如下，修訂目的是加強保安措施及符合相關監管要求，以保障客戶資料及交易安全。

條款	**內容（刪除之內容以劃掉方式標記，新增及更改之內容以灰色標記）**
條款名稱	328 營商網上理財保安認證服務之條款及細則
2	認證服務能讓閣下在指定型號流動裝置*上儲存的生物認證記錄或自訂保安密碼透過大新銀行 328 營商流動應用程式（「該應用程式」）(i) 登入大新銀行 328 營商流動理財服務（「流動理財」）~~及／或大新 328 營商網上理財服務（「網上理財」）~~；及(ii) 透過互聯網，或本行認可之其他電子媒介給予本行指示及向本行作出申請（以取代（在本行綜合章則及條款中定義的）保安編碼）。 *指定型號流動裝置為本行不時指定並可與該應用程式及認證服務相容的流動電子裝置。請聯絡本行取得最新的指定型號流動裝置名單。
5	閣下知悉並同意若閣下透過流動理財及大新 328 營商網上理財服務（「網上理財」）使用認證服務：
5.2	閣下必須在指定型號流動裝置安裝最新版本的該應用程式；
5.4	閣下需要透過流動理財~~輸入以 SMS 短訊發送到閣下已登記於本行的流動電話號碼之一次性密碼~~登記認證服務；
5.7	**處理個人信息的目的及方式：**閣下同意及授權本行可聘用第三方服務供應商及其關聯公司和要求相關政府機關（統稱「資料處理方」）為身份驗證目的在香港特別行政區和中國內地（視乎情況而定）使用和處理閣下就驗證閣下及／或閣下於本行 328 營商網上理財服務的用戶之身份而提供的身份驗證資料（包括但不限於任何照片及圖像）和銀行紀錄（如適用），及傳輸驗證結果予本行。
5.8	閣下在此確認，並基於本行已明確告知以下內容，就第 5.7 條所述的特定處理行為給予如下單獨同意： (i) **關於處理《中華人民共和國個人信息保護法》及相關法律法規所規定的敏感個人信息**：閣下知曉並單獨、明確地同意，本行為履行第 5.7 條所述的身份驗證流程，將處理閣下及／或閣下的用戶之如下敏感個人信息 — 該等敏感個人信息的具體範圍包括但不限於：身份證件中所載信息（包括晶片、姓名、性別、出生年月日、住址、民族、公民身份證號碼、簽發機關、有效期限和通行證號碼）、閣下及／或閣下的用戶現場拍攝的面部照片、動態視頻（如適用）、人臉識別特徵。 (a) 必要性說明：收集此類敏感個人信息是進行遠程真人驗證及防範欺詐風險的必要技術手段。如果不提供，閣下及／或閣下的用戶將無法通過網上渠道完成身份驗證。

	(b) 對權益的影響：本行及資料處理方將採取嚴格的安全措施保護該等信息。一旦洩露或非法使用，可能導致閣下及 / 或閣下的用戶的人格尊嚴受到侵害或人身、財產安全受到危害。 (c) 保存期限：僅在驗證目的所需的最小範圍內查閱個人資料，並在驗證完成後及適用的法律法規規定的期限內刪除相關資料。 (ii) **委託處理及向第三方資料處理方提供個人信息**：閣下知曉並單獨、明確地同意，為實現第 5.7 條所述之目的，本行將向本行不時受託的第三方資料處理方（包括但不限於中華人民共和國公安機關及其他相關政府機關（統稱「公安機關」））提供閣下及 / 或閣下的用戶之個人信息，由有關資料處理方協助處理上述信息。 (iii) **關於跨境提供個人資料**：閣下知曉並單獨、明確地同意，為實現第 5.7 條所述之目的，本行將閣下及 / 或閣下的用戶之個人資料傳輸至本行及資料處理方位於中國內地及香港特別行政區（視乎情況而定）的伺服器及 / 或資料處理方進行如下方式的存儲及處理，閣下知悉該等跨境提供行為可能存在的相關風險以及行使個人權利之途徑。 (a) 處理方式：接收加密的個人信息，連接公安機關數據源核驗用戶身份信息的真實性，返回驗證結果。 (b) 數據保存期限及閣下的權利：資料處理方僅在驗證目的所需的最小範圍內查閱個人資料，並在驗證完成後及適用的法律法規規定的期限內刪除相關數據；本行將根據反洗錢及相關法律規定的期限保存驗證記錄。 (c) 行使個人權利之途徑：如閣下 / 或閣下的用戶需要向資料接收方行使查閱、複制、更正或刪除個人信息的權利，可直接聯系資料接收方或聯系銀行處理。 (iv) **免責與風險提示：**閣下同意資料處理方閣下提供的資料之取用及使用不能構成閣下對銀行作任何投訴、申索、索求、訴訟理由或法律程式的任何基礎。 (v) **免責與風險提示：**閣下知悉本行進行的網上身份驗證是由人工智慧（AI）技術驅動並存在風險，該系統可能會錯誤地拒絕為持有真實身份的閣下及 / 或閣下的用戶進行驗證，導致閣下及 / 或閣下的用戶未能成功完成身份驗證。閣下亦同意，如閣下及 / 或閣下的用戶未能成功完成上述驗證，閣下及 / 或閣下的用戶可能需要致電本行的客戶服務熱線或親身到本行的任何分行進行身份驗證。
6.	縱使本行提供認證服務，閣下仍可選擇使用閣下的集團編號、用戶編號、密碼及使用 SMS 短訊一次性密碼透過該應用程式登入流動理財及透過瀏覽器登入網上理財。然而，為保障閣下的戶口安全，本行建議閣下於已登記認證服務的流動裝置使用生物認證或自訂保安密碼認證登入流動理財。
~~10~~	~~如閣下使用 QR 碼去登入網上理財：~~
~~10.1~~	~~閣下需使用該應用程式內置的掃瞄器；~~

~~10.2~~	~~閣下需於 QR 碼產生的 100 秒或其他指定時間內完成整個登入程序。如未能完成，閣下需重新整理頁面或等待原有的 QR 碼到期，以獲得新的 QR 碼。~~
~~11~~10	本行建議閣下於閣下的指定型號流動裝置允許接收該應用程式~~接收~~發出的推送通知，否則閣下不會收到由該應用程式發出的通知，從而未能使用部分認證服務。
~~16.2~~15.2	閣下在其他流動裝置就同一流動理財~~帳~~賬戶登記認證服務；
~~16.3~~15.3	~~閣下的自訂保安密碼被連續錯誤輸入 5 次~~閣下已超過本行允許的自訂保安密碼認證及 / 或生物認證嘗試次數上限，因而未能成功登入流動理財及 / 或授權交易；
~~16.4~~	~~閣下已經累積 5 次臉部識別失敗；~~
~~16.5~~15.4	閣下要求停用認證服務；或~~。~~
15.5	閣下的身份驗證未能通過本行的複查，
~~17~~16	如閣下有雙胞胎或長相相似的兄弟姊妹，則不應使用 Face ID 認證或臉部識別，建議閣下使用本行允許的自訂保安密碼認證~~保安編器~~以登入流動理財、~~及~~網上理財及其它本行不時~~所~~支援~~或將會~~的應用程式。Face ID 認證及臉部識別的面孔辨識錯誤機率可能會因應特定情況而有所不同，例如雙胞胎、長相相似的兄弟姊妹或青少年，以及閣下裝置設定中「使用臉部識別需要注視螢幕」的功能被停用。如閣下仍然希望使用 Face ID 認證及 / 或臉部識別，請閣下承擔相關風險和後果。

閣下有權終止大新銀行有限公司 (「本行」) 所提供之保安認證服務 (「有關服務」)，藉此拒絕接受有關修訂。若閣下於生效日或之後仍繼續進入最新版本的 328 營商流動應用程式及 / 或使用有關服務，則有關修訂對閣下具有約束力。請注意，若閣下不接受有關修訂，本行將可能無法繼續為閣下提供有關服務。

本通知的中英文版本如有歧異，概以英文版本為準。

大新銀行有限公司
2026 年 1 月

大新銀行
DAH SING BANK

Notice of Amendments relating to Terms and Conditions for the Security Authentication Service of 328 Business Banking

With effect from 25 January 2026 ("Effective Date"), the Terms and Conditions for the Security Authentication Service of 328 Business Banking will be amended as follows. The amendments aim to enhance security measures and comply with relevant regulatory requirements to protect customer data and transaction safety.

Clause	Content (deletion is crossed out, addition and changes are shaded in grey)
Name of T&C	Terms and Conditions for the Security Authentication Service of 328 Business e-Banking
2	The Service (i) provides you an alternative means to log into 328 Business Mobile Banking Service ("Mobile Banking"); ~~and / or 328 Business e-Banking Service ("e-Banking");~~ and (ii) allows you to (instead of using the Security Code (defined in the Master Terms and Conditions of the Bank)) give instructions and make applications to the Bank through the Internet or other electronic means acceptable to the Bank via our 328 Business Mobile Application (the "App") by using your biometric authentication record(s) stored on your designated mobile device* or self-assigned security passcode. *Designated mobile device means a mobile device which is compatible to the App and Service as may be announced by us from time to time. Please contact us for the updated list of such designated mobile devices.
5	You acknowledge and agree that in order to use the Service through Mobile Banking and / or 328 Business e-Banking Service ("e-Banking"):
5.2	You must install the latest version of the App on a designated mobile device;
5.4	You must register the Service through Mobile Banking ~~by using the one-time password sent to your mobile number registered with our Bank~~;
5.7	**Purpose and manner of processing personal information:** You consent to and authorise the Bank to engage third-party service providers and their affiliates, and, where necessary, request relevant government authorities (collectively, the "Data Processors") to use and process the identity verification data you provide for the purpose of verifying your identity(ies) and/or the identity(ies) of your users of the Bank's 328 Business e-Banking services in the Hong Kong Special Administrative Region and Chinese Mainland (as the case may be), including but not limited to any photos and images, and bank records (if applicable), and to transmit the verification results to the Bank.
5.8	You acknowledge and, based on the Bank's clear disclosure of the following, provide the following separate consents regarding the specific processing activities described in clause 5.7: (i) **Regarding the processing of sensitive personal information as defined under the Personal Information Protection Law of the People's Republic of China and related laws and regulations**: You acknowledge, and explicitly and separately consent that, to perform the identity verification processes described in clause 5.7, the Bank will process the following sensitive personal information - the specific scope of such sensitive personal information includes but is not limited to information contained in identification documents (including chip, name, gender, date of birth, address, race, national ID number, issuing authority, validity period, and passport number), live facial photos, dynamic videos (if applicable) and facial recognition features taken on-site by you and/or your users. (a) Necessity: Collecting such sensitive personal information is a necessary technical means to conduct remote in-person verification and prevent fraud risk. If not provided, you and/or your users will not be able to complete identity verification via online channels. (b) Impact on rights and interests: The Bank and the Data Processors will take strict security measures to protect such information. In the event of leakage or illegal use, it may result in infringement upon your or your users' personal dignity or pose a threat to personal and property safety.

	(c) Retention period: Personal data will only be accessed to the minimum extent necessary for verification purposes and will be deleted after the verification is completed and within the time limits prescribed by the applicable laws and regulations. (ii) **Entrusted processing and provision of personal information to third parties**: You acknowledge, and explicitly, separately consent that, to achieve the purpose described in clause 5.7, the Bank may provide your personal information to the third-party Data Processors entrusted by the Bank from time to time (including but not limited to the Public Security Bureau of the People's Republic of China and other relevant government authorities (collectively referred to as the "Public Security Bureau")), who will assist in processing the aforementioned information. (iii) **Regarding the cross-border provision of personal data**: You are aware of, and explicitly and separately consent that, for the purposes described in clause 5.7, the Bank may transfer your or your users' personal data to servers and/or the Data Processors located in Chinese Mainland and the Hong Kong Special Administrative Region (as the case may be) for storage and processing in the following manner. You acknowledge the potential risks associated with such cross-border transfers and the means to exercise personal rights. (a) Processing method: Receive encrypted personal information, verify the authenticity of the user's identity information by connecting to the Public Security Bureau's data sources, and return the verification results. (b) Data retention period and your rights: The Data Processor will only access personal data to the minimum extent necessary for verification purposes and will delete the relevant data after verification is completed and in accordance with the period specified by the applicable laws and regulations; the Bank will retain verification records according to anti-money laundering and related legal requirements. (c) Personal rights: If you or your users wish to exercise the right to access, copy, correct, or delete personal information with the data recipient(s), you or your users may directly contact the data recipient(s) or contact the Bank for handling. (iv) **Disclaimer and risk notice**: You agree that the use of your data by the Data Processors cannot serve as any basis for complaints, claims, lawsuits, demands, grounds for litigation or legal proceedings against the Bank. (v) **Disclaimer and risk notice**: You are aware that the Bank's Online Identity Verification is driven by artificial intelligence (AI) technology and carries risks. The system may erroneously refuse to verify you and/or your users who possess(es) genuine identity(ies), resulting in your failure and/or the failure of your users to complete identity verification. You also agree that, if you and/or your users fail to complete the above verification, you and/or your users may need to call the Bank's Customer Service Hotline or visit any branch of the Bank in person for identity verification.
6	You may still choose to log into Mobile Banking via the App and e-Banking via Internet browsers with Group ID, User ID, password and a SMS one-time password notwithstanding our provision of the Service. However, to ensure the security of your account, we recommend you to log into Mobile Banking on the mobile device through which the Service has been registered, with biometric authentication or self-assigned security passcode authentication.
~~10~~	~~If you use QR code to login e-Banking:~~
~~10.1~~	~~you must use the scanner provided in the App;~~
~~10.2~~	~~you must complete the login within 100 seconds or such other designated time period upon the appearance of the QR code. If you fail to do so, you should refresh the page or wait until the original QR code expires to receive a new QR code.~~
~~11~~10	We recommend you to allow receiving push notifications ~~for~~ from the App on your designated mobile device. Otherwise, you will not be receiving notifications from the App and may not utilize certain part or parts of the Service.
~~16.3~~15.3	~~you fail to input self-assigned security passcode for 5 consecutive times;~~

	you have exceeded the maximum number of attempts as permitted by the Bank for self-assigned security passcode authentication and/or biometric authentication and thereby failing to log into Mobile Banking and/or authorize transactions;
~~16.4~~	~~you have accumulated 5 times of facial recognition failure;~~
~~16.5~~15.4	you instruct the Bank to do so;~~. or~~
15.5	you fail the identity re-verification conducted by the Bank, ~~You~~ and you are required to re-register for or re-activate the Service.
~~17~~16	You should not use face ID authentication or facial recognition if you have an identical twin sibling or a sibling who looks like you, in which case you should use ~~other form of approved authentication~~ the self-assigned security passcode authentication as permitted by the Bank to access Mobile Banking, e-Banking and any other mobile applications that we may support from time to time. The probability of a false match using face ID authentication and facial recognition varies in some cases, such as for twins or siblings who look alike or adolescents, and the disabling of "Require Attention for Facial Recognition" function from your device settings. Please accept the associated risks and consequences if you continue to enable the face ID authentication and / or facial recognition.

Please note that you may refuse to accept the above amendments by terminating the security authentication service provided by Dah Sing Bank, Limited ("Bank") ("Service"). Otherwise, the above amendments shall be binding on you if you continue to access to the latest version of 328 Business Mobile Application and/or use the latest version of the Service on or after the Effective Date. Please also note that the Bank may not be able to continue to provide you with the Service if you do not accept the above amendments.

In the event of any inconsistency between the English and Chinese versions of this document, the English version shall prevail.

Dah Sing Bank, Limited
Jan 2026