Personal Information and Privacy Protection Policy (applicable to Mobile Banking)

Issuance Date: 22 Nov 2025
Effective Date: 22 Nov 2025

Hang Seng Bank (China) Limited ("Hang Seng", "the Bank", "we" or "us"), with the register office 34/F, 36/F & 46F, Hang Seng Bank Tower, 1000 Lujiazui Ring Road, Free Trade Zone, Shanghai, China, take personal information confidentiality and security very seriously, and strive at all times to protect our customers' and related parties' personal information and privacy when we provide our good services with you. We therefore formulate this Personal Information and Privacy Protection Policy **(applicable to Mobile Banking)** (this "Policy") to comply with the laws, regulations, rules and regulatory requirements.

Important Notice: This Policy applies to your use of our mobile banking services. If there is any discrepancy between this Policy and the other agreements entered into or other terms and conditions agreed between you and us, such other agreements or terms and conditions shall prevail. You agree and understand the Bank may collect, store, use, process, transfer, provide, disclose, delete or use other methods to process your personal information.

If you have any query, comment or suggestion, please contact us. You may contact us through below contact detail or "contact us" which is stated in our official website （www.hangseng.com.cn） or mobile device application.

Contact Us: DATA PRIVACY OFFICER（DPO)

https://www.hangseng.com.cn/1/2/contact-us-chi/email-us

Hotline：400 830 8008

This Policy include below content：

CNX750-R3(YX) 1-21 10/25E

I. Personal Information and Privacy Protection Policy Overview – How We Protect Your Personal Information

1. Overview

To preserve the confidentiality, security and privacy of all personal information you provide to us, we follow the principle of reasonableness, legitimacy rightfulness and honest, and adopt below principle of public and transparent to protect and process your personal information:

(1) We only collect personal information that we believe to be relevant and required for us to comply with law, perform a statutory responsibility or statutory obligation, understand your service needs, build up, review, maintain and develop our relationship with you, provide you with materials of relevant products and services.

(2) We may for specific purposes provide your personal information to other members of the HSBC Group, our agents or other third parties, as permitted by law. We will obtain your consent to comply with the laws.

(3) We will not transfer or provide your personal information to any third party, unless it is made to comply with law, perform a statutory responsibility, statutory obligation or perform the agreement, or in accordance with this Policy or other agreement between you and the Bank.

(4) We may be required from time to time to disclose your personal information to our regulators, other governmental or judicial bodies or agencies, but we will only do so following the requirement of law, performance of statutory responsibility, requirement of regulator and government, performance of statutory obligation or agreement to the extent that we deem necessary.

(5) We will not publicly disclose your personal information and we will obtain your separate consent and inform you the purpose, style and method of the personal information which is publicly disclosed.

(6) We aim to keep your personal information on our records accurate and up-to-date. You can contact us to modify or supplement as per the contact detail stated in this Policy.

(7) We maintain strict security systems and perform necessary inspection and filing procedure to comply with laws to prevent unauthorised access to your personal information by anyone.

(8) All members of the HSBC Group, all our staff and all third parties with permitted access to your personal information are specifically required to take necessary measures to ensure the process of personal data is equivalent to the standard of personal information protection as stipulated in this Policy.

By maintaining our commitment to these policies, we will ensure that we respect the inherent trust that you place in us.

CNX750-R3(YX) 2-21 10/25E

2. Information Security

(1) Information security is our top priority. We will endeavour at all times to safeguard your personal information against unauthorised or accidental access, processing or damage. We maintain this commitment to information security by implementing appropriate security and managerial measures to secure your personal information.

(2) We will strictly comply with the requirements of "Measures for the Administration of Electronic Banking" to keep the personal information provided by the users and customers of the Bank's mobile banking confidential and store such personal information securely. To enable you to use the Bank's mobile banking safely, we will provide the bank level information protection. The Bank's mobile banking will be accessed to by using encryption mode (such as HTTPs and TLS) and the transfer and encryption of the relevant data should be conducted under the Bank's security standard so as to satisfy the bank level security requirements.

(3) We have a dedicated team for business management, technology support and security protection to operate and manage the Bank's mobile banking services. The team has clear and specific responsibilities for information security and the team leader will ensure these responsibilities to be performed. In addition, the Bank also sets up a series of management mechanism for system access, data privacy and security safeguard.

(4) The servers of the Bank's mobile banking services are deployed in the unified data center of our Group. We effectively prevent network attacks by properly setting up and using the firewall and antivirus applications within a highly secured environment. In addition, we catch all abnormal status through real-time monitoring system, such as low disk space, IP attack etc., which will trigger system alerts to administer and security team by SMS and emails to ensure the fast response.

(5) We exercise strict management over our staff members who may have access to your personal information, including but not limited to access control applied to different positions, contractual obligation of confidentiality agreed with relevant staff members, formulation and implementation of information security related policies and procedures, and related training offered to staff. When we use services provided by external service providers (entities or individuals), we also impose strict confidentiality obligations on them and request them to abide by our security standards when processing personal information.

(6) **For the security of your personal information, you take on the same responsibility as us. You shall keep your personal information secret and confidential, such as your account information, identity information, identity verification information (e.g. user name, password, dynamic password, verification code, activation code, etc.), and all the documents, devices or other media that may record or otherwise relate to such information, and shall ensure your personal information and relevant documents, materials, devices or other media are used only in a secured environment. You shall not, at any time, disclose to any other person or allow any other person to use such information and relevant documents, devices or other media. Once you think your personal information and/or relevant documents, devices or other media have been disclosed, lost or stolen, or may otherwise affect the security of your use of our products, devices or services, you shall notify us immediately so that we may take appropriate measures to prevent further loss from occurring.**

(7) If unfortunately, personal information security incident occurs, we will adopt emergency plan and take relevant actions and remediation measures to mitigate the severity and losses in connection therewith. Meanwhile, we will, following the applicable requirements set out in law and regulation, inform you of the basic information of the security incident and its possible impact, the actions and measures we have taken or will take, suggestions for you to prevent and mitigate the risk, and applicable remediation measures. We will inform you about the security incident by email, mail, call, SMS, push notification or through other methods as

appropriate in a timely manner. Where it is difficult to notify each Personal Information Subject, we will post public notice in a reasonable and effective way. Meanwhile, we will report such personal information security incident and our actions in accordance with applicable law, regulation and regulatory requirements.

II. How we collect your personal information

1. Personal information refers to any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized. Personal information include name, birth date, ID certificate information (ID card, passport and etc.,), personal biometrics recognition, information, contact information, address, account information, property status, location and etc., Sensitive personal information refers to personal or property information that, once leaked or illegally provided or misused, may harm personal or property safety and will easily lead to infringement of the personal reputation, human dignity, physical or psychological health, or discriminatory treatment. Such information mainly includes ID certificate information (ID card, passport and etc.,), personal biometrics recognition, bank account, credit information, property information, transaction information, location, medical and health, biometrics recognition, specific identity, financial account, as well as any personal information of a minor under the age of 14.

The processing of sensitive personal information has a significant impact on your personal rights and interests. Once leaked or illegally used, it may endanger your personal and property safety. We will carry out information processing activities in accordance with laws, regulations, regulatory requirements and your agreement, and take appropriate security measures to protect your personal information. If you refuse to provide such sensitive personal information or do not have the participation of such sensitive personal information, our bank will not be able to provide you with specific products or services, nor supervise and manage the daily business operations.

2. For the purpose of complying with law, regulation and regulatory provision, or as required for us to provide you with various products and services and continuously improve our products and services , or in order to contact or communicate with you, understand the needs of you, build up, review, maintain and develop our relationship with you, we may receive and keep the personal information provided by yourself, or, according to law, regulation, regulatory provision, your authorisation or consent, collect, enquire, and verify by proper methods from/with members of the HSBC Group or other third parties (including but not limited to credit reference agencies, information service providers, relevant authorities, employers, counterparties, joint applicants, contact persons, close relatives and other entities/individuals).

3. The personal information we collect may be recorded in paper, electronic means (for example, including but without limitation to the information we collect by way of automated machine, website, online banking, mobile banking or other mobile device application, email, short message, push notification, telephone banking or other channels) or any other means.

4. In order to provide you with mobile banking services, fulfil the Bank’s legal obligations and to ensure the safety of our mobile banking services, you need to provide us or allow us to collect from you the following information necessary for the following purposes or functions described in below as well as under Article III of this Policy, "How We Use Your Personal Information ". If you fail or refuse to provide the following personal information, we may not provide certain function of mobile banking services:

(1) Setup for Mobile Bank or reset Mobile PIN

You will need to provide your date of birth and, depending on your choice, your Electronic Banking number and phone banking number, or your debit card number, card issue number and debit card PIN, or your name, Chinese second-generation ID card number and facial biometric information for mobile bank setup;

(2) Logging on mobile bank

You will need to provide your preset Mobile PIN, or Your mobile banking username, logon password, second password, security code and security password pre- set by you or created or sent via security device, mobile phone, other equipment or methods (collectively "password");

(3) Maintaining proper and secure operation of mobile banking, preventing and controlling mobile banking related risks

We may collect **the technical information such as your device type, operating system, unique device identifier, software version, International Mobile Equipment Identity (IMEI), logon IP/MAC address, internet service provider (ISP).** If above information cannot be used to identify your identity or retrieved to personal information, we will not treat it as your personal information. If the information alone or in combination with other information may be used to identify your identity, we will treat it as your personal information and have it properly protected.

If you refuse to provide these information, you will not be able to register or logon our mobile banking service account, or will not be able to use our regular mobile banking services in a safe and normal way.

5. You may decide, at your free choice, to provide us with your personal biological identification information for the following purpose or functions described in below as well as under Article III of this Policy, " How We Use Your Personal Information".

(1) Logon Mobile banking

In order to allow you to logon Mobile banking safely and conveniently, if your device supports biometric authentication, you can choose to activate biometric logon for Mobile banking. Such information is processed and stored by the mobile phone terminals. We only collect the biometric recognition result, rather than keep the raw biometric information. If you do not want to use biometric logon, you can also logon mobile banking via other methods which we provide.

(2) The functions based on fingerprint/facial recognition

In order to allow you to use mobile banking safely, including Mobile Phone Receive Money Settings, update ID information, and update personal information**, we need to collect and save your facial information for retention, auxiliary identification and verification during your business process to ensure your normal use of this service. We may encrypt your facial information and send it to the Ministry of Public Security for verification and accept the verification results. We will store the facial information separately from the personal identity information, and take security measures such as encrypted storage. The retention period is an additional five years from the end of your relationship with our bank. Upon expiration of the above retention period, we will delete or anonymize your personal biometric information and transaction information.**

You have the right to choose whether to provide your facial information or not, but if you chose not, we will not be able to provide you with certain online products or services which are subject to face verification according to the nature of business and/or risk management purpose. Alternatively, you may handle the relevant business/service at our branches.

Facial information is sensitive personal information. For the impact of processing facial information on your personal rights and interests (the impact of sensitive personal information processing activities on your personal rights and interests), please see "II. How we collect your personal information, Article 1".

6. You may decide, at your free choice, to provide us with your personal information for the following functions described in below as well as under Article III of this Policy, " How We Use Your Personal Information ".

(1) Transfer and Remittance

To provide you with transfer and remittance service, we need to collect from you the name of payee, beneficiary bank account number (or card number) and the name of beneficiary bank.

If you want to transfer by using "Mobile Phone Number Transfer" function, you need to provide the payee mobile phone number, the payee name and the name of beneficiary bank(optional).

If you want to set "Mobile Phone Receive Money" function, we need to collect your mobile phone number, your receiving account number, and we will use your facial biometrics information and SMS verification code to verify your identity.

To provide you with overseas transfer and remittance service, we need to collect from you the payee's name and address, the name of beneficiary bank, beneficiary account number, country/region where beneficiary bank is located or transfer purpose.

You need to provide debit card PIN, or security code via security device or SMS verification code, for approving and processing transaction requests or instructions. We will also collect the records of these transactions for your check or enquiry.

We will collect your account balance information for the purpose of notifying you with your account balance update via SMS function or Push Notification function.

(2) Risk Profiling Questionnaire

Your age, family assets, income information, investment experience, investment preference and risk tolerance, planned investment products and tenor.

We will collect the expire date of your Risk Profiling Questionnaire for the purpose of notifying you with expiry reminder via SMS function or Push Notification function.

(3) Purchasing and selling foreign currencies, foreign currencies exchanging, purchase of financial products such as structured deposit and mutual fund

Your name, ID type, ID number, purpose of purchasing or selling foreign currencies.

We will collect your payment transactions information for the purpose of notifying you with your account balance update via SMS function or Push Notification function.

(4) Deposit and Structured Deposit

Your name, ID type, ID number, tax residence, taxpayer identification number.

You need to provide debit card PIN, or security code via security device or SMS verification code for approving and processing transaction requests or instructions. We will also collect the records of these transactions for your check or enquiry.

We will collect your payment transactions information for the purpose of notifying you with your account balance update via SMS function or Push Notification function.

(5) Local Unit Trust Fund，Mutual Recognition Fund, Segregated Account and QDII Products

Your name, ID type, ID number, tax residence, taxpayer identification number, account information (account number, currency type, account balance), funds transaction information and the way of share out bonus, your written signature.

You need to provide debit card PIN, or security code via security device or SMS verification code for approving and processing transaction requests or instructions. We will also collect the records of these transactions for your check or enquiry.

We will collect your payment transactions information for the purpose of notifying you with your account balance update via SMS or APP Push Notification function.
We will collect your payment transactions information for the purpose of notifying you with your account balance update via SMS function or Push Notification function.

(6) Financial Planning Questionnaire

Relevant information will be collected according to the family structure of your choice, includes: year of birth, annual income (family or individual), total loan amount (family or individual), retirement age, post-retirement expenditure (family or individual), estimated education funds for children.

(7) Insurance application

Your Name, Date of Birth, Gender, ID type, ID number, Tax Resident Identity and Account Information (account number, currency type, account balance). According to different insurance products, further information will be collected including the information of the insured and policy holder (Name, Date of Birth, Gender, ID type, ID number, the validity of ID, Nationality, Address, Postal code, Email address and mobile phone number, insured amount, both inured and policy holder's ID Image(both front side and back side) and written signature).

You need to provide debit card PIN, or security code via security device or SMS verification code for approving and processing requests or instructions for insurance transactions. We will also collect the electronic policies for your future enquiry.

We will collect your payee's account number and balance for the purpose of notifying you with your account balance update via SMS function or Push Notification function.

(8) Update the certificate information

Photo of front side and back side of your ID certificate, ID information including your name, ID number, date of birth, effective date and tenor of the certificate.

We will also use your facial biometrics information and SMS verification code to verify your identity.
We will collect the period of validity of your ID Card for the purpose of notifying you with expiry reminder via SMS function or Push Notification function.

(9) Update personal information
Upon the updated information you provided, we will collect your name, nationality, residential information (including residential country/region, residential address, beginning date of your residence, home phone number); mailing information (including mailing country/region, address and postcode(optional)); job information (including your profession, occupation, industry, company's name and address, office phone number(optional), country/region you work, income); and other information (including marital status, education, and email address (optional)).

We will also use your facial biometrics information, debit card PIN, security code via security device or SMS verification code to verify your identity.

(10) CAT I account bind with CAT II account
In order to verify the identity information of the CAT I account cardholder and process your card binding service application, the People's Bank of China Clearing Center Interbank Account Information Authentication Service Platform and Allinpay Network Services Co., Ltd. will verify Your name, Debit Card number of CAT I account, the name of CAT I account bank, mobile phone number, you need to provide SMS verification code to verify your identify.

(11) Alipay Service Setting
Your Name, Debit card number, Alipay account number, mobile phone number, and you need to provide SMS verification code to verify your identify.

(12) Privileges and Reward Mall
When you use reward mall service, your name, reward account status, reward balance and the code of gift coupon will be provided to HUGME MARKETING, Reward Mall service provider (contact phone number is 400-608-1001).

(13) Bank Card and Pinless Setting
Your bank card number, bank account type and number.
You need to provide debit card PIN, or security code via security device or SMS verification code for verifying your identify, approving and processing transaction requests or instructions.

(14) Finding branches nearby
Your geographic location information for showing the nearby branches**.**

(15) Account opening appointment
Your name, title, contact number, city you are living in.

(16) Contact us
Your name, title, contact number, email address, city you are living in, details about what you enquire.

(17) Qualified Investor Certification

We will collect the proof of your assets and investment experience to review whether the materials you submit meet the qualification standards for qualified investors required by regulatory regulations.

(18) Online Service Application Center

Your name, account information (account number, currency type, account balance), contact number, city you are living in, mailing address, details about what you apply.

(19) ECNY Service

Your name, bank account or bank card number, ECNY eWallet ID, ECNY eWallet Name, ECNY eWallet Tier 2.0 operator bank name, mobile phone number, you need to provide SMS verification code to verify your identify.

(20) Notification Center

We will use the software service toolkit provided by Tencent ("SDK").

To provide the Push Notification function to you, **such SDK will collect your related device information.** For details, please refer to 6 Tencent Mobile Push SDK instructions**.**

You can manage whether to allow pop-up notifications through your mobile system ->Settings->Notifications, and you can read or delete the message in our APP "Notification Center".

(21) Foreign-related income declaration

Your name, account information including account number, currency, declared amount, contact number, and the content of the information required to be declared.

(22) CAT II settlement account opening

If you open CAT II settlement account on the Bank's mobile banking, you need to provide your personal identity information (may involving your name, ID type, ID number and the expire date of the ID etc.) , personal basic information (may involving name, gender, birth date, nationality, place of birth, address, family status, mail address, mobile phone number, email address, etc.), personal education and working information (may involving occupation, company name, position, etc.) and the information of the other CAT I settlement account cards you hold.

In order to verify the identity information of the CAT I account cardholder and process your card binding service application, the People's Bank of China Clearing Center Interbank Account Information Authentication Service Platform and Allinpay Network Services Co., Ltd. will verify Your name, Debit Card number of CAT I account, the name of CAT I account bank, mobile phone number, you need to provide SMS verification code and facial biometrics information to verify your identify. We need to collect and save your facial information for retention, auxiliary identification and verification during your business process to ensure your normal use of this service. We may encrypt your facial information and send it to the Ministry of Public Security for verification and accept the verification results. We will store the facial information separately from the personal identity information and take security measures such as encrypted storage. The retention

period is an additional five years from the end of your relationship with our bank. Upon expiration of the above retention period, we will delete or anonymize your personal biometric information and transaction information.

If you refuse to provide the above information, you are not able to use or enjoy the relevant functions, but your use of other functions of our mobile banking will not be adversely affected.

7. In addition, our mobile banking applications may also invite your permissions for the following system functions relating to personal information and will collect and use the information for the permitted functions based on your permission:

Items	Permitted Functions
Fingerprint logon	Identity recognition, logon, and verification using fingerprint(s).
Face ID	Logon mobile banking via facial recognition on some types of device.
Camera	Need to access your camera for face recognition, ID update, ID recognition.
Photos	need to access your photo album to upload your ID to complete identity verification.
Location	Obtain your geographic location to show you nearby outlets. The system background saves your location information during transactions.
Notification	Push notification with alerts, sounds, and icon tags (manage notification on the mobile through System > Settings > Notifications)
Device information	Obtain your device information for sending push notifications.
Storage	Obtain your storage permissions to save your e-statements/e-advice.

For those functions that need your permission, you may, at your free choice, decide whether to additionally grant the permission for the said functions on mobile banking applications. **If you refuse to grant permission for a specific function, you are not able to use that specific function**, but your use of other functions in our mobile banking will not be adversely affected.

For example, APP may support to cancel your previous function permission. You may choose to turn off relevant system permissions, setting path as below:

For Android: Setting-Application-Permissions
For Apple IOS: Setting-Privacy-Permissions-Application

If you cancel the system permissions, we will no longer process relevant personal information. However, the above cancellation would not impact the processing of your personal information based on your previous system permissions.

8. When you use our Mobile Banking Service, under certain particular scenarios, we will use the software service toolkit provided by third party ("SDK"). To provide the service to you, SDK will collect your information:

Third Party	**SDK**	**Scope and purpose of collection**
Automatic Software Co., Ltd.	Map of Gaode, location, Search SDK	To provide the location-based service, we use Map of Gaode, location, Search SDK of Automatic Software Co., Ltd., and SDK needs to obtain your following personal information: IDFA, OAID, GAID, application name, application version number, device brand and model, operating system, operator information, screen resolution, IP address, GNSS information, network type, WiFi status, WiFi parameters, WiFi list, WiFi signal strength information, WiFi gateway address, SSID, BSSID, base station information, sensor information (vector, acceleration, pressure), device signal strength information, longitude and latitude, as well as location, network access, and positioning device permission information. The collection frequency involves acquisition at startup or call, and on-demand. Privacy Policy: https://lbs.amap.com/pages/privacy/
Industrial Digital Financial Services (Shanghai) Co., Ltd.	CibFintech SDK	To quickly verify your identity by obtaining and recognizing your face feature and action. Privacy Policy: https://open.cibfintech.com/portal/private.html
Tencent Computer Systems Company Limited	WeChat SDK	For sharing to weChat, but weChat will not collect your personal information. Privacy Policy: https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_cn&t=weixin_agreement&s=privacy
AppDynamics, Inc.	AppDynamics SDK	To analyze the performance of Mobile Banking, we will use AppDynamics SDK to obtain your mobile IP, mobile manufacturer, mobile type, network type， visit length information. Privacy Policy: https://www.appdynamics.com/legal/privacy-policy
Tealium	Tealium SDK	To do visit statistics survey and client behavior analysis, we use Tealium SDK to access to your mobile IP, mobile manufacturer, network type, browser type, system operation version, system operation type, and pages you visit or click. Privacy Policy: https://tealium.com/privacy/
Tencent Cloud Computing (Beijing) Co., Ltd.	Tencent Push Notification Service(' TPNS') SDK (integrate	To provide Push Notification function, we will use 'TPNS' SDK (Huawei, Honor, vivo, OPPO, Xiaomi device users will use relevant push SDK of the manufacturer, other devices will use 'TPNS' push SDK) to access to your device information (mobile manufacturer, mobile type, Mobile Operating System version and language, mobile network information (IP address, telecom operator, network type,),

	d by Huawei, Xiaomi, Honor, OPPO, VIVO push SDK) Face ID SDK	our APP information (notification bar status, running application process), application data (push, Click and other data), integrate device identification information used by manufacturers (such as IMEI, QAID, Android ID, IDFV).For details, please refer to Privacy Policy: https://cloud.tencent.com/document/product/548/50955 In order to open a CAT II settlement account for the purpose of security verification, compliance responsibilities and risk management, customers need to undergo a facial verification check. Facial Verification SDK Privacy Policy Link: https://cloud.tencent.com/document/product/1007/71390
OneSpan	RASP SDK	To fortify the app and proactively deter users from running the client mobile app on devices with identified security vulnerabilities, we will use OneSpan RASP SDK to access inventory of installed software throughout the utilization of the mobile app. Privacy Policy: https://www.onespan.com/privacy-center
China Financial Certification Center	Yunzhengtong (China Financial Certification Center CFCA) SDK	To provide you with mobile banking setup, login and transaction verification services, the SDK is used for digital certificate issuance, download and electronic signature services. For AIS system SDKs, device information, model number, brand name, system image compilation information sequence, vendors, and chip vendors will be collected. For IOS systems, the SDK collects IP addresses.

If you refuse the listed SDK(s) to collect your information, you may not be able to access these services, but you can still access to other functions or services on mobile banking.

9. To provide with you the loan business, we may use indirect collection to obtain your personal information from third parties, but we will ensure that such indirect collection follows the principle of minimum quantity. We will ask the third party to explain the source of your personal information provided, and confirm the legitimacy of the source of your personal information, and we will check with the third party the scope and purpose it has obtained of your authorization for processing personal information. In addition, the third party shall undertake that it has obtained your full, informed and valid consent (including the separate consent and/or written consent as required by applicable laws). If the personal information processing activities we need to carry out for business are beyond the scope of your authorization to the third party, we will obtain your consent again through the third party.

10. Please understand that the services we provide are constantly evolving. If you choose to use any other service not listed above for which we have to collect your information, we will separately explain to you, the purposes, methods, and scope of personal information we collect, through reminders on pages, interaction with you, agreements entered into with you or other appropriate method, and obtain your consent for that. We will use, store, disclose, and protect your information in accordance with this Policy and other agreements (if any) between you and us. If you choose not to provide certain information, you may be unable to use certain or part of the service, but your use of other services we provide will not be affected.

III. How we use your personal information

1. We will use your information in the following circumstances

(1) To realize the purposes and functions mentioned in above Article II. of this Policy "How We Collect Your Personal Information"; to contact you, or to approve, process, manage, execute or effect your application or instruction for transactions;

(2) To ensure safe and stable financial services, we will use your information for identity verification, safety precaution, fraud detection, prevention or prohibition of illegal or incompliant activities, control or reduction of risks, recording or filing purposes;

(3) To comply with the applicable laws and regulations or discharge of legal duties; to report to relevant regulators or other authorities according to laws, regulations or regulatory requirements;

(4) to maintain and improve mobilebanking business function, and develop new features (if any new feature will use your personal information for any other purpose and scope than you have agreed, we will seek your further consent before launching any of such use);

(5) to investigate and prevent, as regulated by applicable laws, any current, potential or sceptical financial crime activities (including money laundering, terrorist financing, bribery and corruption, tax evasion, fraud, sanction evasion and/or any action or attempt to breach or evade applicable laws and regulations as related), and manage financial crime risk;

(6) to facilitate the internal operation of us or HSBC group (for purposes including credit and risk management, statistics, data analysis and process, system, service, product development and improvement, planning, insurance, audit and management governance);

(7) Subject to your authorization, to promote the Bank's other products and services and to recommend to you the products or services that may interest you;

CNX750-R3(YX) 13-21 10/25E

(8) To make statistics and analysis of the use of our business, products, services or functions; we may share such statistics to the public or third parties to present overall trend of relevant business, products, services or functions. But such statistics will not contain any of your personal identifiable information.

2. The above content related to information collection and use in this Policy shall not impact our use of your information for the purposes as otherwise agreed between you and us separately.

3. If we use your personal information for the purposes other than the purposes of information collection and use as set forth in this Policy or in other agreement between you and us, we shall let you know how we use this information and obtain your consent before using your personal information for such additional purposes as per applicable laws and regulations.

IV. How we share, transfer your personal information

1. Entrusted Processing and Sharing

(1) Unless otherwise agreed by you in express, we will not share with, publish or disclose any of your personal information to any third party other than HSBC group member. Only for legislative, reasonable, necessary and specific purpose will we provide related personal information of yours to a third party. When we entrust a third party to process your personal information, we will have binding contract with the third party on the purpose, term, methodology, information type, information security measures, etc., and monitor the third party activities as related to information process. Further delegation will not be allowed by us before we have your prior consent.

(2) For the purposes set out above in this Policy, we may provide or disclose all or part of your personal information to the following recipients under the preconditions that such provision or disclosure is necessary and is made with proper protective measures provided that we or the recipients inform you of the name of recipient, contact information, purpose of disposal, the type of information that will be disposed and you grant specific consent to do so, and in case any of your personal information is to be disposed in any other methodology or for any other purpose, we will seek your further consent in advance (unless any of such specific consent is exempted by law):

(a) a member of the HSBC Group (for instance, we may engage another HSBC group member to dispose your personal information so as to extend the availability of our service to you);

(b) any contractor, subcontractor, agent, third party product or service provider, licensor, professional consultant, business partner, or associated person of the HSBC Group (including their employees, directors and officers) (for instance, we may provider telecom service provider with **your mobile phone number, transactional type, transaction amount and account balance information** so that the telecom service provider could inform you of such information);

(c) any regulator of the Bank or any member of the HSBC Group or any other authority, or any organisation or individual designated by such regulators or authorities;

(d) anyone acting on your behalf according to your authorisation or according to law, payment recipients, beneficiaries, account nominees, correspondent and agent banks (e.g. for CHAPS, BACS, SWIFT, CIPS and CNAPS), clearing houses, clearing or settlement systems, anyone making any payment to you;

(e) any person or related party who has the right or obligation, acquires an interest or assumes risk, in or in connection with any product or service you receive from the Bank, or any business

CNX750-R3(YX) 14-21 10/25E

you handle at the Bank or any transaction you make with the Bank (for example, the person who provides or intends to provide any mortgage or other security for any of your debt to the Bank, or the beneficiary of the insurance product that the Bank distributes to you);
(f) other financial institutions, industrial associations, bank card organizations, credit rating agencies, credit reference agencies (including without limitation, the People's Bank of China's credit information database) and information service providers (for instance, we may provide credit reference agencies with such information as related to your application for loans and performance of repayment, to facilitate objective reflection of your credit status);
(g) any third party fund manager providing you with asset management services or insurance companies providing you with insurance services (for instance, we will provide your account information to finance institutes from which you have obtained assets management service or insurance service so as for the institutes to identify your payment);
(h) any third party that provides us with referral, agency or intermediary service, or to whom we provide referral, agency or intermediary service;

2. **Transfer**

We will not transfer your personal information to any other company, organization or individual, except for the following,

(1) Where in compliance with applicable law, upon your request we will transfer in such manner that is available by us, to the recipient you designate;
(2) in the case of business/asset transfer, restructure, disposal (including securitization), merger, spin-off, acquisition transactions, dismissal or bankruptcy of us where the transfer of your personal information is necessary. **In such cases, we will inform you of the identity and contact method of the personal information recipient as per applicable laws and regulations as well as request said recipient to comply with this Policy. If the personal information recipient changes the purposes and methods of personal information processing activities under this Policy, it shall re-obtain the consent from you.**

V. How we store and cross border transfer your Personal Information

1. In principle, the personal information we collected and generated in our domestic operation will be stored within the territory of People's Republic of China (the "PRC").

2. However, as part of a global financial institution, we provide products or services through globally deployed resources and applications. We also accept the products and services from the HSBC Group and its vendors, or conduct other business with them. Therefore, to realize the purposes described in this Policy and other relevant legal documents, we will cross-border transfer your personal information to offshore jurisdictions where HSBC Group and its vendors are located or be subject to visits from these areas or jurisdictions. We will provide your personal information to overseas recipients subject to applicable laws and regulations, and notify you of the name and contact information of the overseas recipients, the purposes and methods of processing, the types of personal information processed, and the methods and procedures for exercising your rights subject to applicable laws or regulations to overseas recipients. For details, please refer to the List for Personal Information Cross-border Transfer (Individual Version)(see [https//:www.hangseng.com.cn/1/PA_esf-ca-app-content/content/pws/home/pdf/NLforPIC_en.pdf] for details). **The List for Personal Information Cross-border Transfer (Individual Version) is in addition to this Policy and, together with this Policy, forms a complete set of rules for us to process your personal information.**

3. **We will take necessary measures to your personal information provided to offshore and request offshore recipient to abide by our personal information protection standard stipulated to comply with laws, regulations and this Policy**.

VI. Special Circumstances for Information Processing

We will process your personal information (such as information collection, storage, use, analysis, transfer, provision, disclosure) based on your consent. To the extent allowed by laws and regulations, we may process your personal information without your consent under the following circumstances:

1. **where it is necessary for entering into a contract or the performance of a contract to which you are the party;**
2. **where it is necessary for compliance with a legal obligation to which we are subject;**
3. **where it is necessary in order to protect your or others' vital interests related to life and property in an emergency or respond to public health emergencies;**
4. **where it is within reasonable limits in order to carry out news coverage or media supervision for the public interest;**
5. **where it is within reasonable range according to law to process the information which has been legally made public or publicized by yourself; or**
6. **other circumstances stipulated by laws and regulations.**

VII. How We Use Cookies and Other Technologies

1. Your visit, browse, use of any website or mobile device application of the Bank may be recorded for analysis on the number of visitors to the site and general usage patterns, helping you reduce the number and frequency of information entry or assisting determine the security status of your account. Some of this information will be gathered through the use of Cookies. Cookies can enable us to provide safer and more useful features for website or application users. The information collected by Cookies is unidentified aggregated research data, and contains no name or address information or any information that will enable anyone to contact you via telephone, email or any other means. Most browsers and/or applications are initially set to accept Cookies. You can manage or delete Cookies as per your preference. Should you wish to disable Cookies, you may do so by changing the setting on your browser and/or application. However, by disabling them, you may not be able to take full advantage of our website and/or application.

2. The website and/or application may also work with third parties to research certain usage and other activities on the website and/or application. These third parties include without limitation to Adobe, etc. They use technologies such as Cookies etc. to collect information for such research. They use the information collected through such technologies (i) to find out more about users, including user demographics and behavior and usage patterns, (ii) for more accurate reporting and (iii) to improve the effectiveness of our marketing. They aggregate the information collected and then share it with us. No personally identifiable information about you is collected or shared by Adobe with us as a result of this research. Should you wish to disable the Cookies associated with these technologies, you may do so by changing the setting on your browser and/or application. However, after changing the setting you may not be able to enter certain part(s) of our website and/or application.

CNX750-R3(YX) 16-21 10/25E

VIII. Your Rights relating to Personal Information

1. You have the right to request us to protect and secure your personal information in accordance with the provisions of the applicable laws and this Policy. You have the right to exercise your rights of individual granted by applicable laws and regulations.

2. You have the right to check with us whether we hold your personal information as well as to access and copy your personal information.

3. You have the right to change the scope of authorization or withdraw your consent(XI. How to Contact Us). We will not further process the related information once you change your authorization. Please note the withdrawal of consent will not affect the lawfulness of processing based on consent given by you before its withdrawal.

4. You have the right and obligation to update your personal information at the Bank to ensure all information be accurate and up-to-date. You have the right to require the Bank to provide convenience for you to update your personal information at the Bank and to correct any of your information that is inaccurate.

5. In relation to personal credit or guarantee, you have the right to request to be informed of your personal information that is disclosed to credit reference agencies by us, so as to enable your request to the relevant credit reference agencies for access to and correction of your information.

6. We will only retain your personal information within the time limit necessary to achieve the purpose of our bank's services and within the time limit allowed by applicable laws, regulations or separately agreed between our bank and you, unless otherwise required or allowed by the applicable laws. If we will respond to your request of deletion in accordance with applicable laws or regulations, we will also notify the third party which obtained your personal information from us and request them to delete such information in a timely manner, unless otherwise stipulated by laws or regulations, or if the third party has obtained your separate authorization.

When we delete your personal information from our service system, your personal information which stored in backup system might be hard to delete at the same time,
However, we assure to delete your personal information when next backup system updates immediately. If one of the following occurs, we will delete your personal information on our own initiative or at your request, unless to comply with the requirements of applicable laws, archives, accounting, auditing and reporting, or to perform the other agreement between you and us, or to clean up the credit and debt relationship between you and us, or to provide information inquiry to you, regulators or other organs to delete your personal information:

(1) the service purpose of the bank has been realized, cannot be achieved or no longer necessary to provide the service;
(2) the bank ceases to provide services, or the storage period has expired or exceed;
(3) you withdraw your consent to us in accordance with the contact information stipulated in the Policy;
(4) we violate laws or regulations or this Policy to deal with your personal information.

7. When you use the mobile banking applications provided by us, you have the right to uninstall the mobile banking applications or stop using the mobile banking applications to refuse us to further obtain your personal information. Please note that to uninstall the mobile banking applications will not close your digital banking account. **You have the right to close your digital banking account (by closing your bank account or disabling the mobile banking functions of your bank account, for the sake of account safety you should visit our branches or sub-branches in person for such closure. If you hold CAT II settlement account with us, please call 24- hour customer service hotline at 4008-30-8008 for closing your bank account after all funds has been transferred out.) and request for deletion of your personal information in accordance with the applicable law and regulation, this Policy, and other agreement between you and us, we will handle your request within 15 working days after receiving your request. After you close your digital banking account, we will no longer collect your information through relevant channel, and will delete relevant personal information in accordance with the applicable law and regulation, this Policy, and other agreement between you and us.**

8. Nothing in this Policy will shall limit the other rights you should have as a Personal Information Subject under applicable laws and regulations.

IX. How to Contact Us

1. Requests to access, copy, transfer, correct, supplement, delete, and restrict the processing of personal information, change/withdraw of authorisation or dispose of personal information beyond retention period, for a copy of this Policy, enquiries about our practices regarding personal information and privacy protection, or exercising other rights you are granted by the applicable laws and regulations, should be addressed to:

https://www.hangseng.com.cn/1/2/contact-us-chi/email-us

Hotline：400 830 8008

"Contact US" on the HANG SENG China APP

our branches or sub- branches

Upon the receipt of your request, we will handle your request and reply to you within 15 working days.

2. For security purpose, you may need to raise your request in written form or use other methods to prove your identity. We may request you to verify your identity before processing your request.

3. Normally the Bank will not charge fees for the processing of your above-mentioned reasonable requests related to personal information. Nevertheless, for the frequently repeated and unreasonable requests, the Bank will charge certain fees as the case may be to the extent allowed by the law and regulation.

Notwithstanding the foregoing, we may reject your request if it is illegal, noncompliant, or unnecessarily repeated, needs excessive technical means (for example, the need to develop information systems or fundamentally change current practices), brings risks to the legitimate rights and interests of others, is unreasonable or technically impracticable.

We may not be able to respond to your request under any of the following circumstances:

(1) where the request is in relation to our legal and financial compliance obligation under laws and regulations;

(2) where the request is in direct relation to state security or national defence security;

(3) where the request is in direct relation to public security, public sanitation, or major public interests;

(4) where the request is in direct relation to criminal investigations, prosecutions, trials, execution of rulings, etc.;

(5) where there is sufficient evidence that you are intentionally malicious or abuse your rights;

(6) where the purpose is to protect you or other individual's life, property and other substantial legal interests but difficult to acquire your consent;

(7) where responses to your request will give rise to serious damage to your or any other individual or organisation's legal rights and interests; or
(8) where the request involves any trade secret.

4. You may supervise or make suggestions for our practices regarding personal information and privacy protection, and lodge complaints or demand compensation according to law against us or our staff for any infringement of your rights and interests in your personal information and privacy. This Policy will be governed by the laws of the People's Republic of China. Any disputes related to this Policy shall be resolved by consultation. If it could not be resolved, you agree the disputes shall be submitted to the People's Court of Pudong New District, Shanghai.

X. How We Handle Minors' Personal Information

1. Using our products and services by minors must be carried out under the supervision of their parents or guardians. We will abide by laws and regulations, this Policy and Provisions on the Cyber Protection of Personal Information of Children to give special protection to minor's personal information. If you are a parent or guardian of a minor, when you have any questions about the information processing of the minor under your guardianship, please contact us through the contact method stipulated in this Policy.

2. We understand the importance of protecting the minors' personal information with extra caution. If you are under 18 years old, it is suggested that your parents or guardians shall carefully read this Policy and you shall submit your personal information only after seeking consent from them. Meanwhile, it is suggested that your use of our product and service is conducted under the guidance of your parents or guardians. If they do not agree you to submit your personal information or to use any product or service of the Bank, you shall immediately stop submitting your information or using the product and service of the Bank. In addition, please notify such event to us as soon as possible, so as to allow us to take effective measures.

3. If you are under 14 years old, you should and only obtain the consent of your parents or guardians to use any product or services of the bank or provide your personal information to the bank. We will process with personal information of minors in accordance with Provisions on the Cyber Protection of Personal Information of Children and with the permission of laws and regulations and the explicit consent of your parents or guardians. If we find ourselves are processing personal information of minors without the consent of verifiable parents or guardians, we will try to delete such personal information as soon as possible.

XI. Update of this Policy and Others

CNX750-R3(YX) 19-21 10/25E

1. This Policy (including the List for Personal Information Cross-border Transfer (Individual Version)) may be amended or updated from time to time. We will publish such changes at our website and/or relevant applications. You should keep an eye on relevant releases from time to time. We also will inform you of the contents of the publication by means of short message, push notification and telephone notification as appropriate. And such amendments and updates will take effect from the expiration of the publication period and replace previous relevant contents. **If you don't agree to modify and update the content of this Policy, you should immediately stop using relevant products and services of the bank. If you continue to use relevant products and services, it will be deemed that you agree to accept the modification. Change of this Policy should not unreasonably reduce or restrict your rights as the personal information subject according to the applicable laws.**

CNX750-R3(YX) 20-21 10/25E

2. If you provide the personal information of other third parties to the Bank, we have the right to know the legitimacy of the source of the information and you have obtained authorization of the third party for us to process the personal information for specific purposes. If we need to process the personal information of the third party to carry out business beyond the scope of authorization of the third party, we will obtain the separate consent of the third party again through you. You should ensure that the third party is aware of this Policy (including the List for Personal Information Cross-border Transfer (Individual Version)) and its subsequent updates from time to time, should specifically inform the third party how the Bank will process its personal information in accordance with this Policy and should ensure that you have obtained the full, informed and valid consent of the third party (including the separate consent and/or written consent as required by applicable laws). You may remind the person to read this Policy beforehand, or you may provide a copy of this Policy to the person.

3. When you accept specific products or services provided by a third party through the products or services of our bank, you confirm that the products or services provided by the third party are operated independently by the third party. The third party shall independently assume full responsibility for the disputes arising from the handing of your personal information by the third party, and we will do our best to assist you in business. If a third party processes your personal information when providing you with products or services, you and the third party shall reach a separate agreement in according with applicable laws.

4. The policy is subject to the Chinese version, and the English translation (if any) is for reference only.

CNX750-R3(YX) 21-21 10/25E