Reminder: To borrow or not to borrow? Borrow only if you can repay!

Terms and Conditions

For Hong Kong Used Only

Please read the terms and conditions below carefully. By using this BOC Connect mobile app ("this service") and the materials from time to time available through this service ("these materials"), you agree to be bound by these terms and conditions. As these terms and conditions may be amended from time to time at the discretion of Bank of China (Hong Kong) Limited (the "Company") and be posted on this service, you should read them again carefully whenever using this service. You are assumed to have agreed to the revised terms and conditions if you continue to use this service following any changes to these terms and conditions.

These terms and conditions are in addition to the license agreement agreed between you and the relevant software providers (including Google Play™ store, App Store and Huawei AppGallery) for use of the Service (the "License Agreement"). In case of any inconsistency or conflict between the License Agreement and these terms and conditions, the latter shall prevail.

These Terms are also applicable for instructions and/or enquiries relating to the Corporate Customer and its accounts given by you as a user and these Terms, as the context may require, shall extend to and be binding on such Corporate Customer and accounts.

Availability

Products and services mentioned in these materials are not available to all persons in all geographic locations. Only persons who are permitted by applicable law may browse the information and/or subscribe the services and products offered. Persons browsing these materials are required to ensure that they are aware of and observe all relevant restrictions that apply to them and are responsible for satisfying themselves that they may do so under the laws or the jurisdiction to which they are bound or located. Eligibility of any person for particular product or service is subject to the final determination of the Company.

Remarks: Google Play logo is a trademark of Google Inc., the App Store is a service mark of Apple Inc., and Huawei AppGallery is provided by Huawei Services (Hong Kong) Co., Limited.

Disclaimer

The information contained in these materials is for general information only and is provided on an "as is" basis without warranty of any kind (including without limitation, merchantability, title,

fitness for particular purpose, freedom from computer virus, non-infringement, compatibility, security, accuracy and completeness) and may be withdrawn and/or changed at any time without prior notice.

This service and/or these materials may not be available at all times and there may be delays, failures, errors or omissions or loss of transmitted information.

No information contained in these materials should be regarded as an offer or solicitation to sell, to subscribe to, or provide any recommendation to any person. The information is not intended to be relied upon as the basis for any decision which may affect you or your business. All persons should consult their own professional adviser before making any investment, financial decision or purchasing any product or subscribing any service.

The Company will endeavour to ensure the accuracy and reliability of the information provided but do not guarantee its accuracy or reliability and accept no liability (whether in tort or contract or otherwise) for any loss or damage arising from any inaccuracies or omissions.

To the extent permitted by applicable law, the Company disclaims liability for any error, omissions or inaccuracies in the information contained in these materials and for any loss or damages, resulting from its use or reliance, or inability to use, by any party or in connection with any error, interruption, delay in operation or incomplete transmission, line or system failure or computer virus. The Company is not responsible in any manner for direct, indirect, special, incidental or consequential damages arising out of the use of this service and/or these materials.

Your use of this service and these materials is entirely at your own risk. The Company does not represent or warrant that no viruses or other destructive properties will be transmitted or that no damage will occur to your equipment or mobile phone. You are solely responsible for adequate protection and back up of data and/or equipment and for undertaking reasonable and appropriate precautions to scan for computer viruses or other destructive properties and to prevent, safeguard and ensure that no computer virus enters your equipment or mobile phone. The Company makes no representations or warranties concerning the accuracy, functionality or performance of any third party software that may be used in connection with this service.

Continued use of GPS running in the background can dramatically decrease battery life.

Terms and conditions for featured / offer sessions:

1. All materials and contents contained in the featured / offer sessions, including but not limited to text, photographs, video, logos, charts and other materials are the property of the Company / content providers, and are protected by copyright or other intellectual property

rights. None of such material and content shall be copied, reproduced or modified.

2. The Company / content providers has the right to remove any information from the featured / offer sessions without prior notice.
3. Information provided in the featured / offer sessions are for reference only. The Company / content providers make no warranty, including but not limited to any warranty on or in relation to the following matters and shall not be responsible or liable for any losses incurred under all circumstances:
    a. the accuracy of the contents of the featured / offer session;
    b. the stability or availability of the featured / offer sessions; and / or
    c. the services or products available from the featured / offer sessions.
4. The securities, commodities, foreign exchanges, derivatives or investments referred to in the featured / offer sessions may not be suitable to you. No consideration has been given to any particular investment objectives or experience, financial situation or other needs of any reader. Accordingly, no representation or recommendation is made and no liability is accepted with regard to the suitability or appropriateness of any of the securities and/or investments referred to herein for any particular person's circumstances. You should understand the nature and risks of the relevant product and make investment decision(s) based on your own financial situation, investment objectives and experiences, willingness and ability to bear risks and specific needs; and if necessary, should seek independent professional advice before making any investment decision(s). The featured / offer sessions are not intended to provide any professional advice and should not be relied upon in that regard.
5. The Company / content providers shall not be liable for any losses which you have suffered or you may suffer as a result of your use or misuse of the featured / offer sessions or your reliance of any information or content from the featured / offer sessions.
6. You shall indemnify the Company / content providers any loss, including but not limited to legal costs and expenses incurred by your misuse of the featured / offer sessions.
7. The Company has the right to amend the terms and conditions herein and you shall be bound by such amendments.

Security Information

This Mobile App provides an one-stop information and service platform for SMEs. You can search "BOC Connect" for free download of the App in the online App stores (Google Play, App Store, and Huawei AppGallery). Do not install mobile Apps from mistrusted sources. If there is any suspicious App, please do not download, login and should stop operation immediately.

Avoid using Mobile Apps via wireless networks (i.e. Wi-Fi) which is public or without password setting. We advise using encrypted and reliable mobile internet connections especially for financial transactions.

Disable any wireless network functions (e.g. Wi-Fi, Bluetooth, NFC) or Payment Apps when not in use. Choose encrypted networks when using Wi-Fi and disable Wi-Fi auto connection setting.

Please do not connect your mobile device to any suspicious computer infected by virus; at the same time, it is recommended to install anti-virus software and setup the firewall in your mobile. Don't use Mobile Apps via any jailbroken iPhone or rooted Android mobile to avoid any potential security loophole. Also, you can download the appropriate mobile security Apps from the online App stores. You can visit HKCERT website for reference: https://www.hkcert.org/mobile-security-tools, to select the appropriate Apps.

To protect your online transactions, we will check whether your mobile device is jailbroken or rooted and with recommended operating systems for minimum security requirements upon using of this Mobile App. Customer may not be allowed to access the Internet Banking Services via such device. Please pay attention to the reminder.

Activate the auto-lock function of your mobile device. Do not use easy-to-guess personal information, numbers or words as your password and avoid using the same password that you have used for accessing other web services.

Upon the successful registration of the “Biometric Authentication” on your mobile phone, any biometric credential that is stored on your mobile phone can be used for the purpose of the “Biometric Authentication”. You must ensure that only your biometric credential is stored on your mobile phone to access the device, and ensure the security of the security codes as well as the password or code that you can use to store your biometric credential and register the “Biometric Authentication” on your mobile phone. For security reasons, do not register biometric credential of other person(s) on your mobile phone or use jailbroken or rooted mobile phone.

You can enable / disable the “Biometric Authentication” through “My Account > Biometric Authentication ” in BOC Connect after login. Please note that after you have disabled the “Biometric Authentication”, your biometric credential will be continuously stored on your designated mobile device. You may consider cancelling the data at your own decision.

You must not use Biometric Authentication if you have reasonable belief that other people may share identical or very similar biometric credential(s) of you or your biometric credential(s) can be easily compromised. For instance, you must not use facial recognition for authentication purpose if you have identical twin or triplet sibling(s).

You must not use Biometric Authentication if the relevant biometric credential(s) of you are or will be undergoing rapid development or change. For instance, you must not use facial recognition for authentication purpose if you are an adolescence with facial features undergoing rapid development.

You will use all reasonable care to keep your mobile phone secure. You will notify us as soon as reasonably practicable if you find or believe that your mobile phone has been lost or stolen or that any unauthorised transactions have occurred.

Please download and install updates and patches for this Mobile App and the other Mobile Apps, operating systems and browsers regularly in the online App stores (Google Play, App Store and Huawei AppGallery) or our website.

Hyperlinks

Use of hyperlinks to other internet sites or resources are at the browser's own risks. The Company expressly disclaims any responsibility for the accuracy or availability of the information provided by those sites or for the safety of information which the browser may provide to any third party. Please visit the following website for full details: http://www.bochk.com/en/hyperlinkpolicy

Copyright

Collection of Information

The Company focuses on its duty of confidentiality to its customers. Please refer to the "Data Policy Notice" for the Company's general policies on collection, use, disclosure and transfer of customer data. For the Company’s policies and practices in protecting personal data privacy,

please refer to the “Privacy Policy Statement". "Data Policy Notice" and “Privacy Policy Statement" are available at https://www.bochk.com.

The Company will record the information of users using the Company's Mobile Application through the Mobile Application server access log (including the clicking date and time, IP address, pages clicked, device, operating system and Advertising Identifier (if applicable)). The Company might use the users’ record of using the Company’s Mobile Application for the purposes of improving the operation of the Mobile Application, conducting statistical analysis and marketing. The Company will keep the relevant information for an appropriate period of time based on the actual needs. The Company’s Mobile Application server access log will record the users’ information automatically by default. Save where express consent or permission is required, by continuing to use the Company’s Mobile Application, users are deemed to have given their consent for the Company to store and use the relevant information in the above manner. If the users do not consent to the above, the users should not continue to use the Company’s Mobile Application and should not provide the user’s relevant information.

(If applicable) The Advertising Identifier is a unique identifier provided by the mobile device’s operating system when the user uses the Company’s Mobile Application. The Advertising Identifier is an anonymous users’ identifier and contains no name, address information nor any information that will enable anyone to contact the users via any means. No user’s personal data will be collected or stored by the Company. Should users wish to disable the Advertising Identifier, they may do so by changing the relevant setting on the mobile device (generally found under ”Privacy” or “Ads” in the mobile device’s settings). The Company may entrust third-party agencies (such as website or mobile application analytics companies) to analyse information of users’ other online activities (including preferences and usage patterns) through the use of users’ Advertising Identifier. Such information may be analysed together with the personal data collected by the Company to enable the Company to understand more about users’ preferences for the purposes of statistical analysis and improving marketing efficiency. The Company will not provide any personal data (which could identify the identity of users) with these third-party agencies or collect any personally identifiable information from these third-party agencies for the foregoing purposes.

Reject of receiving notification and direct marketing

BOC Connect may send push notification and / or personalized notification via In App Notification, eDM, SMS, if you do not wish to receive notification and direct marketing, you can do so by:

1. put "✓" on the box of “BOC Connect will collect your personal data for direct marketing purposes by providing you with news update on SME related products and services from Bank of China (Hong Kong) Limited ("the Bank'). If you **DO NOT** wish to receive direct marketing from the platform, please put "✓" on this box.”; or

2. turn off “Receive Push Notification” and “Receive Personalized Notification” under the session of “More”.

Governing Law

These terms and conditions are governed by the laws of the Hong Kong Special Administrative Region. The parties submit to the non-exclusive jurisdiction of the Hong Kong courts.

Language

The Chinese version of these terms and conditions is for reference only. If there is any conflict or inconsistency between the Chinese and the English version, the latter shall prevail.

Risk Disclosure Statements

Investment involves risks. Terms apply. For details and relevant investment risk factors, please contact the staff of BOCHK.

Conditions for Services

By using our Mobile Banking Services, you have confirmed your acceptance of our Conditions for Services (as amended by us from time to time). Please visit the following website for full details: http://www.bochk.com/en/conditions

Other Term

If any part of these terms and conditions shall be deemed unlawful or for any reason unenforceable, then that provision shall be deemed to be severable from these terms and conditions and shall not affect the validity and enforceability of any of the remaining provisions of these terms and conditions.

Terms and Conditions for use of biometric authentication for BOC Connect of Bank of China (Hong Kong) Limited

1. These terms and conditions ("Terms") apply to and regulate your use of biometric authentication for BOC Connect of Bank of China (Hong Kong) Limited (“the Bank" or “we” or “BOCHK”). By registering or using biometric authentication for the Bank's BOC Connect, you are deemed to accept and agree to these Terms. If you do not accept these Terms, please stop registering or using biometric authentication for the Bank's BOC Connect.

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 BOC Connect, to authorize instruction in respect of transactions as specified by the Bank from time to time through the Bank's BOC Connect or to do such other things or transactions as notified by the Bank from time to time. Designated mobile device means iPhone® 5s or higher, specified models of Samsung or LG and such other electronic equipment that we may enable for use with biometric authentication from time to time and includes the operating system or software that the device operates on. Please contact us for the updated list of such electronic equipment.

3. You agree that BOCHK may treat and consider as valid and binding on you any instruction given, or agreement made with BOCHK, which is authenticated through biometric authentication without BOCHK making any further inquiry as to the authority or identity of the person making or purporting to give such instructions or to make such agreement or their authenticity notwithstanding any error, misunderstanding, fraud, forgery or lack of clarity in the authorization. You acknowledge that BOCHK may still require you to authenticate a transaction by your password and/or another form of authentication even though you have authenticated the same by your biometric credential(s).

4. These Terms are in addition to and shall be read in conjunction with the Bank's Conditions for Services and any other documents forming part of our banking agreement (and any reference to the terms and conditions of the Conditions for Services shall include reference to these Terms). The Conditions for Services may be accessed at http://www.bochk.com/en/conditionsforservices.html. 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.

5. You acknowledge and agree that in order to use biometric authentication for the Bank's BOC Connect:

a. You must be a valid user of our Mobile App services;

b. You will need to activate the relevant biometric authentication function on your designated mobile device and register at least one of your biometric credentials to control access to this service;

c. You must register the biometric authentication through the Bank's BOC Connect and choosing to use the relevant biometric credential(s) that you stored on your designated mobile device for the purpose of biometric authentication;

d. You understand that upon the successful registration of the biometric authentication on your designated mobile device, any biometric credential(s) that is/are stored on your designated mobile device can be used for the purpose of the biometric authentication. You must ensure that only your biometric credential(s) is/are stored on your designated mobile device to access this service;

You must not use the biometric authentication if you have reasonable belief that other people may share identical or very similar biometric credential(s) of you or your biometric credential(s) can be easily compromised. For instance, you must not use facial recognition for authentication purpose if you have identical twin or triplet sibling(s);

e. You must not use the biometric authentication if the relevant biometric credential(s) of you are or will be undergoing rapid development or change. For instance, you must not use facial recognition for authentication purpose if you are an adolescence with facial features undergoing rapid development;

f. You should ensure the security of the security codes as well as the password or code that you can use to store your biometric credential(s) and register the biometric authentication on your designated mobile device; and

g. You will use all reasonable care to keep your designated mobile device secure. You will notify us as soon as reasonably practicable if you find or believe that your designated mobile device has been lost or stolen or that any unauthorised transactions have occurred.

6. You acknowledge that the authentication is performed by the Bank's mobile app by interfacing with the biometric authentication module on the designated mobile device and you agree to the authentication process. The Bank will not collect/store your biometric credential(s) in any manner at any stage of your registration or use of the biometric authentication for the Bank's BOC Connect.

7. You can disable the biometric authentication for the Bank's BOC Connect by yourself at any time on the Bank's BOC Connect once you are login. Please note that disabling of the biometric authentication for the Bank's BOC Connect will not automatically delete your biometric credential(s) on your designated mobile device. Your biometric credential(s) will be continuously stored on your designated mobile device unless they are deleted by you through the relevant biometric authentication function on your designated mobile device. Biometric credential(s) stored on your designated mobile device may be used by other applications on your designated mobile device. You may consider to cancel the data at your own decision.

8. If your biometric credential(s) or other security code of the designated mobile device has been compromised, you are required to change the security code, re-register your biometric credential(s) or cease the use of the biometric authentication for the Bank's BOC Connect.

9. You and the Corporate Customer that you are acting for and on behalf of will be liable for all losses if you and/or the Corporate Customer have acted fraudulently or with gross negligence, or allowed any third party to use your designated mobile device, password and/or authentication tool, or failed to comply with your obligations under these Terms, the Conditions for Services, the Security Information and other relevant documents as provided by the Bank from time to time. You would not otherwise be responsible for any direct loss suffered by you as a result of unauthorised transactions conducted through your account.

10. In addition to and without subtracting the disclaimers and exclusions of liability in the

Conditions for Services:

a. You understand that the biometric authentication module of the designated mobile device is not provided by the Bank, and we make no representation or warranty as to the security of the biometric authentication function of any designated mobile device and whether it works in the way that the manufacturer of the device represents.

b. We do not represent or warrant that the biometric authentication for the Bank's Mobile Banking will function at all times or with any electronic equipment, software, infrastructure or other Internet Banking that we may offer from time to time.

c. You and the Corporate Customer that you are acting for and on behalf of shall indemnify us and keep us indemnified against any consequences, claims, proceedings, losses or damages whatsoever and howsoever caused (save and except any direct loss or damages caused by negligence or misconduct on the part of us) that may arise to be incurred by us and against any costs and expenses (including all legal costs on an indemnity basis) of reasonable amount reasonably incurred by us in making biometric authentication available to you and/or the Corporate Customer arising in connection with any improper use of the biometric authentication.

d. 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.

Note: iPhone is a trademark of Apple Inc.

Privacy Policy Statement

The purpose of this Privacy Policy Statement is to establish the policies and practices of BOC Hong Kong (Holdings) Limited and its subsidiaries, including Bank of China (Hong Kong) Limited, BOC Credit Card (International) Limited, BOC Group Life Assurance Company Limited, Po Sang Securities and Futures Limited, BOCHK Asset Management Limited (each a "Company", for so long as such Company remains a subsidiary of BOC Hong Kong (Holdings) Limited and notwithstanding any change in the name of the Company) towards the Company’s commitment in protecting personal data privacy in accordance with the provisions of the Personal Data (Privacy) Ordinance (the "Ordinance"). The Company highly values personal privacy and strives to preserve the confidentiality and security of all the personal information

which the Company may collect so as to strengthen the trust and confidence between the Company and the Data Subjects, Employees, Users and Other Individuals (as hereinafter defined).

The term "Data Subject(s)", wherever mentioned in this Statement, includes the following categories of individuals:

a. applicants for or customers, authorized signatories, insured persons, policy holders, beneficiaries and other users of financial, insurance, credit card, securities, commodities, investment, banking and related services and products and facilities and so forth provided by the Company;

b. sureties, guarantors and parties providing security, guarantee or any form of support for obligations owed to the Company; and

c. directors, shareholders, officers and managers of any corporate applicants and Data Subjects/users.

The term "Employee(s)", wherever mentioned in this Statement, includes employees and/or applicants for any openings offered by the Company.

The term "user(s)", wherever mentioned in this Statement, includes visitors and/or users of the Company's Website, or when the visitors and/or users communicate with the Company via any electronic devices including but not limited to computer and mobile phone ("Electronic Devices").

The term “Other Individuals”, wherever mentioned in this Statement, include suppliers, contractors, service providers, business partners, landlords, tenants, participants of seminars, visitors, other contractual counterparties of the Company and the employee(s) of the above-mentioned parties (if applicable).

For the purposes of this Statement, the "Group" means the Company and its holding companies, branches, subsidiaries, representative offices and affiliates, wherever situated. Affiliates include branches, subsidiaries, representative offices and affiliates of the Company's holding companies, wherever situated.

The rights and obligations of each Company under this Statement are several and not joint. No Company shall be liable for any act or omission by another Company.

Kinds of Personal Data Held

There are three broad categories of personal data held in the Company. They comprise personal data contained in the following:

1. **Data Subject records**, which are necessary for Data Subjects to supply to the Company from time to time:
    a. in connection with the opening or continuation of accounts and the establishment or continuation of banking facilities or provision of financial, insurance, credit card, securities, commodities, investment, banking and related services and products and facilities;

    b. in the ordinary course of the continuation of the relationship between the Company and Data Subjects, for example, when Data Subjects write cheques, deposit money, effect transactions through credit cards issued or serviced by the Company or generally communicate verbally or in writing with the Company.

2. **Employee records**, which include but are not limited to the name, address, e-mail address, contact phone number, educational background, curriculum vitae and relevant personal data of family members of Employees.

3. **Other Individuals records,** which include but not limited to the name, address, e-mail address, contact phone number of suppliers, contractors, service providers, business partners, landlords, tenants, participants of seminars, visitors, other contractual counterparties of the Company and the employee(s) of the above-mentioned parties (if applicable); and other operational and administrative records that contain personal data.

Purpose of Keeping Personal Data

1. In relation to Data Subjects:

The purposes for which the data relating to the Data Subjects may be used are as follows:

a. assessing the merits and suitability of the Data Subjects as actual or potential applicants for financial, insurance, credit card, securities, commodities, investment, banking and related services and products and facilities and/or processing and/or approving their applications, variation, renewals, cancellations, reinstatements and claims;

b. facilitating the daily operation of the services, credit facilities provided to and/or insurance policies issued to the Data Subjects;

c. conducting credit checks whenever appropriate (including, without limitation, at the time of application for credit and at the time of regular or special reviews which normally will take place one or more times each year) and carrying out matching procedures (as defined in the Ordinance);

d. creating and maintaining the Company's scoring models;

e. providing reference;

f. assisting other financial institutions to conduct credit checks and collect debts;

g. ensuring ongoing credit worthiness of Data Subjects;

h. researching, customer profiling and segmentation and/or designing financial, insurance, credit card, securities, commodities, investment, banking and related services and products and facilities for Data Subjects' use;

i. marketing services, products and other subjects (please see further details in paragraph 10 of the Company's Data Policy Notice ("DPN"));

j. determining amounts owed to or by the Data Subjects;

k. enforcing Data Subjects' obligations, including without limitation the collection of amounts outstanding from Data Subjects and those providing security for Data Subjects' obligations;

l. complying with the obligations, requirements or arrangements for disclosing and using data that apply to the Company or any of its branches or that it is expected to comply according to:

    i. any law binding or applying to it within or outside the Hong Kong Special Administrative Region existing currently and in the future (e.g. the Inland Revenue Ordinance and its provisions including those concerning automatic exchange of financial account information);

    ii. any guidelines or guidance given or issued by any legal, regulatory, governmental, tax, law enforcement or other authorities, or self-regulatory or industry bodies or associations of financial services providers within or outside the Hong Kong Special Administrative Region existing currently and in the future (e.g. guidelines or guidance given or issued by the Inland Revenue Department including those concerning automatic exchange of financial account information);

    iii. any present or future contractual or other commitment with local or foreign legal, regulatory, governmental, tax, law enforcement or other authorities, or self-regulatory or industry bodies or associations of financial services providers that is assumed by or imposed on the Company or any of its branches by reason of its financial, commercial, business or other interests or activities in or related to the jurisdiction of the relevant local or foreign legal, regulatory, governmental, tax, law enforcement or other authority, or self-regulatory or industry bodies or associations;

m. complying with any obligations, requirements, policies, procedures, measures or arrangements for sharing data and information within the Group and/or any other use of data and information in accordance with any group-wide programmes for compliance with sanctions or prevention or detection of money laundering, terrorist financing or other unlawful activities;

n. enabling an actual or proposed assignee of the Company, or participant or sub-participant of the Company's rights in respect of the Data Subjects to evaluate the transaction intended to be the subject of the assignment, participation or sub-participation;

o. comparing data of Data Subjects or other persons for credit checking, data verification or otherwise producing or verifying data, whether or not for the purpose of taking adverse action against the Data Subjects;

p. maintaining a credit history or otherwise, a record of Data Subjects (whether or not there exists any relationship between Data Subjects and the Company) for present and future reference; and

q. purposes incidental, associated or relating to the abovementioned purposes.

2. **In relation to employees (as and where applicable):**

The purposes for which the data relating to the Employees may be used in connection with the employer and employee relationship and human resources management, including but not limited to the purposes as mentioned herein:

a. processing employment application;

b. determining and reviewing salaries, bonuses and other benefits should be employed;

c. conducting reference check with previous employers;

d. consideration for promotion, transfer or secondment;

e. monitoring compliance with internal rules of the Company;

f. any other purposes directly or indirectly relating to the compliance by the Company or any of the employment or statutory obligations; and

g. administering any affairs or benefits relating to the retirement and insurance plan of Employees.

3. **In relation to Other Individuals(as and where applicable):**

   The purposes for which the data relating to the Other Individuals may be used are as follows:

   a. engaging, managing, monitoring and assessing the business relationship with the suppliers, contractors, service providers, business partners and their staff who provide services to the Company;

   b. managing, monitoring and assessing the landlord and tenant relationship with the landlords and/or tenants;

   c. organizing and delivering seminars for the Company; and

   d. facilitating the daily operation and administration of the above.

Collection and Use of Personal Data

1. In relation to the collection of the personal data, the Company will provide the Data Subjects with a copy of the DPN and/or (as and where applicable) the Employees with a copy of relevant Notice in connection with the collection of Employee records and/or (as and where applicable) will notify Other Individuals of the purpose of collection, classes of persons to whom the data may be transferred, their rights to access and correct the data, and other relevant information.

2. In relation to the collection of the information and personal data on-line or when the Users communicate with the Company via Electronic Devices, the following provisions shall be applicable to the Company's Website or when the Users communicate with the Company via the Electronic Devices:

   a. This section is limited to the information collected on the Company's Website, the Company's online advertisements and electronic communications. This section does not apply after the Users leave the Company's Website or when the users visit third-party's websites where the Company's online advertisements are displayed or links to third-party websites not operated or controlled by the Company.

   b. By browsing the Company's Website, electronically responding to the Company's online advertisements, communicating with the Company via any Electronic Devices, the Users' consent to the Company's use of cookies and the Company's use of the Users' Information in the manner as set out in this section. The Users do not proceed further and do not provide the Information unless the Users' consent to the above.

c. The Company will record the information of visitors visiting the Company's Website through the web server access log (including the clicking date and time, IP address, pages clicked, browser type, device, operating system and Internet Banking account number (if applicable)). The Company might use the Users' record (and may combine with other personal information of the Users) for the purposes of improving the operation of this website, statistical analysis and marketing. The Company will keep the relevant information for an appropriate period of time based on the actual needs. The Company's web server access log will record the Users' information automatically by default. By continuing browsing the Company's Website, users are deemed to have given their consent for the Company to store, use and transfer the information in the above manner. The Users' visit to the Company's Weixin Official Account may be recorded. The Company may also provide the record of users' visit to Weixin Official Account above to BOC Credit Card (International) Limited for statistical purpose and for analysis on the number of users and general usage patterns. Some of the Users' information including Users' personalized settings information will be gathered through the use of "cookies". Cookies are small bits of information that are automatically stored in the web browser in Users' Electronic Devices that can be retrieved by the Company's Website. The information collected by "cookies" is anonymous visitor's personalized settings information and contain no name or address information or any information that will enable anyone to contact the Users via any means. No Users' personal data will be collected or stored by the Company. For Internet Banking and Mobile Banking services, a "cookie" with a unique identifier assigned by the Company will be stored in the Users' web browsers throughout the session after login. Cookies will be expired upon logging off. Should the Users wish to disable these cookies, the Users may do so by changing the setting of the browser. However, the Users will then not be able to login the Company's Internet Banking and Mobile Banking services.

d. There are sections of the Company's Website and Weixin Official Account where the Company specifically asks for the Users' personal data, for example, when completing online forms to submit an enquiry, applying for a particular product or service or if registering to use the online services, such as Internet Banking and Mobile Banking services. Please refer to and read the applicable terms and conditions for these products and services as well as the DPN informing the types of data collected, purposes of collection, classes of persons to whom the Users' data may be transferred, the rights to access and correct the personal data, and other relevant information. If the Users do not consent

to the same, please do not proceed further and do not provide the Users' personal data to the Company and Weixin Official Account.

e. Personal data collected by the Company through the Company's Website in connection with an application for employment (as and where applicable) will be used to assess the suitability of the applicant to the job application. The Company may collect the applicant's basic personal data including the name, e-mail address, contact phone number, educational background and curriculum vitae. Please refer to and read the relevant Notice in connection with Employee records when making job application through the Company's Website. Failure to supply such data may result in the Company being unable to process the applicant's employment application.

f. For the purpose of Mobile Application services, unless the context otherwise requires, references in this Statement to "the Company's Website" shall be read as reference to "the Company's Mobile Application".

g. When Users using the Company's Mobile Application services and the Company's Weixin Official Account services , the Company may access the Users' location data to search for the nearest ATM, branch or to conduct valuation of a nearby property. For Mobile Application services, the Company may also access the following of the Users' Electronic Devices: (i) installation identification number (ii) location data, (iii) microphone, (iv) camera, (v) phone book, (vi) calendar, (vii) biometric authentication module and (viii) speech recognition of the Users' Electronic Devices to provide the related Mobile Application services. However, the location, calendar, biometric data and the related information would not be stored or recorded in the database of the Company. If there is an SD card available to the Users' Electronic Devices, the Company may access the SD card for amending or deleting encrypted application data stored in the SD card so as to enable the operation of the Company's Mobile Application services. Users who do not allow the Company to use the information in the above manner may at any time change the setting of the Electronic Devices or uninstall the Mobile Application or unfollow the Company's Weixin Official Account. In such event, Users may only be able to partially use or may not be able to use the Company's Mobile Application or Weixin Official Account services.

h. For "e-Wallet" application, the Company may collect and store the unique identifier of the user's mobile phone (i.e. IMEI number), of mobile phone SIM card and/or of "e-Wallet" application to enable the handset matching and service eligibility checking for the purpose of operating the mobile payment

services. Users who do not allow the Company to use the information in the above manner may at any time uninstall the "e-Wallet" application. In such event, Users will not be able to use the Company's "e-Wallet" application services.

i. After the Users follow the Company's Weixin Official Account, the Company will access the Users' Open ID, Profile Photo, Nickname, Gender, Country/Region/City, Follow/binding time and status of the Users' Weixin Official Account from Weixin platform automatically for the purpose of pushing notification message, statistical and analysis purposes. The Company may also provide the information above to service provider(s) for the purposes of verifying User's identity and pushing correspondent reply message (e.g. lucky draw result), if necessary. Users who do not allow the Company to use the information in the above manner may at any time unfollow the Company's Weixin Official Account. In such event, Users may not be able to use the Company's Weixin Official Account services.

j. Except for Internet Banking, Mobile Banking services, Commodities Internet Trading services, online forms, Mobile Application and Weixin Official Account services where the Company specifically asks for the Users' personal data, the Users can use the Company's Website without providing any of the Users' personal data.

Retention of Personal Data

The personal data and information provided by Data Subjects and/or the Employees and/or the Users and/or Other Individuals will not be kept longer than necessary for the fulfillment of the purposes for which the personal data and information are or are to be used at the time of the collection and for compliance with the legal, regulatory and accounting requirements from time to time.

Disclosure of Personal Data

The personal data and information would not be disclosed to other parties unless such disclosure is made in accordance with DPN and/or (as and where applicable) the relevant Notice in connection with the collection of Employee records and/or the Data Subjects and/or the Employees and/or the Users and/or Other Individuals have been previously consented to and/or the disclosure is permitted or required by any law binding on the Company.

Security of Personal Data

The personal data and information provided to the Company are secured with restricted access by authorized personnel. Encryption technology is employed for sensitive data to protect the privacy of the Data Subjects, the Employees, the Users and Other Individuals during data

transmission.

If the Company engages service providers to handle or process personal data (whether within or outside Hong Kong) on the Company's behalf, the Company would adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the service providers for processing.

Changes to the Privacy Policy Statement

The contents of this Statement may be amended from time to time. Please approach the Company and/or visit the Company's Website regularly for the Company's latest privacy policy.

Data Access Requests and Data Correction Requests

The Company would comply with and process all data access and correction requests in accordance with the provisions of the Ordinance.

The Company may impose a reasonable fee for complying with a data access request in accordance with the Ordinance.

Contact Details

The persons to whom requests for access to data or correction of data or for information regarding policies and practices and kinds of data held are to be addressed are as follows:

Bank of China (Hong Kong) Limited

The Data Protection Officer
Bank of China (Hong Kong) Limited
Bank of China Tower
1 Garden Road
Hong Kong
Facsimile: +852 3717 4635

BOC Credit Card (International) Limited

The Data Protection Officer
BOC Credit Card (International) Limited
15/F, BOC Credit Card Centre
68 Connaught Road West
Hong Kong
Facsimile: +852 2541 5415

BOC Group Life Assurance Company Limited

The Data Protection Officer
BOC Group Life Assurance Company Limited
13/F, 1111 King's Road, Taikoo Shing
Hong Kong
Facsimile: +852 2522 1219

Po Sang Securities and Futures Limited

The Data Protection Officer
Po Sang Securities and Futures Limited
4/F, BOC Yuen Long Commercial Centre
102-108 Castle Peak Road, Yuen Long
New Territories, Hong Kong
Facsimile: +852 2905 1909

BOCHK Asset Management Limited

The Data Protection Officer
BOCHK Asset Management Limited
5/F, Bank of China Building
2A Des Voeux Road Central
Hong Kong
Facsimile: +852 2532 8216

If there is any inconsistency between the English version and the Chinese version of this Statement, the Chinese version shall prevail in relation to any matters arising in the Mainland China exclusive of Hong Kong Special Administrative Region, the English version shall prevail in relation to any matters arising in Hong Kong Special Administrative Region and elsewhere.

January 2022