12. Specific Terms and Conditions for Online Enterprise Banking Services

The additional provisions (*"Terms"*) set out in this section 12 of Part B of the Master TC will apply if a Customer requests internet banking services.

By registering to use or using the Mobile Banking App (as defined hereinafter), the Website (as defined hereinafter) and the Online Enterprise Banking Services (as defined hereinafter), you will be deemed to have accepted and be bound by these Terms, our Privacy Policy and PDPO Notice.

General

12.1 The Existing Terms (as defined hereinafter) shall apply in addition to these Terms. If there is any inconsistency between the Existing Terms and these Terms, the provisions of these Terms shall prevail in relation to the Mobile Banking App, the Website and Online Enterprise Banking Services.

12.2 The Online Enterprise Banking Services are offered to the Customer only in jurisdictions where and when they may be lawfully offered. The Online Enterprise Banking Services and information relating to the Online Enterprise Banking Services are not intended for access or use by persons in other jurisdictions unless such access or use is lawfully permitted. Persons accessing the Online Enterprise Banking Services must be aware of and observe any applicable laws rules and regulations.

Definitions and interpretation

12.3 Unless otherwise defined in these Terms, terms defined in the Existing Terms shall have the same meaning when used herein.

12.4 In these Terms, the following expressions, unless the context requires otherwise, shall have the following meanings:

"**Account**" means any account(s) held by the Customer with the Bank from time to time which is subject to the Existing Terms.

"**App Store**" means any digital distribution platforms designated by the Bank from which the Mobile Banking App is made available for download from time to time.

"**App Store Rules**" means any rules or policies applied by the relevant App Store governing the access to the Mobile Banking App.

"**Authorised Representative**" means:

(a) the individual(s) authorised by the Customer via the Online Enterprise Banking Services Application / Maintenance Form as described below in Clause 12.21 from time to time to use the Online Enterprise Banking Services through the Website or through the Mobile Banking App; and

(b) such other Authorised Persons, officers, employees or agents authorised by the Customer to act on its and/or its affiliates' behalf with respect to the use or operation of the Website or the Mobile Banking App.

"**Authoriser**" refers to the individual(s) nominated by the Master or the Customer via an Online Enterprise Banking Services Application / Maintenance Form (and/or any other form and/or materials as required by the Bank from time to time) and/or the Online Enterprise Banking Services directly and approved by the Bank to do all the things as described below at Clause 12.21(b), which may be amended from time to time.

"**Bank**", in these Terms, has the meaning given to it in the "*Terms and Conditions for Accounts and Related Services (For Enterprise Customers)*" and/or the "*Master Terms and Conditions for Accounts and Services (Business Customers)*" (as the case may be), which expression includes its successors in title, assigns and transferees and any persons deriving title under any of them).

"**Biometric Credential Authentication Service**" has the meaning as defined in the *Terms and Conditions for Mobile Token and Biometric Credential Authentication Service*.

"**Biometric Credentials**" has the meaning as defined in the *Terms and Conditions for Mobile Token and Biometric Credential Authentication Service*.

"**Customer**" means each customer to whom the Bank provides the Online Enterprise Banking Services and, where the context permits, includes any person and Authorised Representative (as the case may be) authorised by the Customer to give Instructions to the Bank in connection with the use of the Online Enterprise Banking Services.

"**Customer Number**" means the unique user short name designated by the Bank for the Customer to access the Online Enterprise Banking Services.

"**Existing Terms**" means, among others, the "*Terms and Conditions for Accounts and Related Services (For Enterprise Customers)*", "*Master Terms and Conditions for Accounts and Services (Business Customers)*", the "*Terms and Conditions for Bank Services relating to Faster Payment System*", the "*Terms and Conditions for Investment Services*", the "*Terms and Conditions in using WhatsApp Chatbot Service*", the "*Terms and Conditions for Mobile Token and Biometric Credential Authentication Service"*, and any other applicable agreements or terms and conditions that the Customer has entered into with the Bank, each as may be amended from time to time.

"**Instruction**" means any instruction given by or on behalf of, or purported to be given by or on behalf of, the Customer to the Bank in relation to any of the Online Enterprise Banking Services.

"**Maker**" refers to the individual(s) nominated by the Customer or the Master via an Online Enterprise Banking Services Application / Maintenance Form (and/or any other form and/or materials as required by the Bank from time to time) and/or the Online Enterprise Banking Services directly and approved by the Bank to do all the things as described at Clause 12.21(c) , which may be amended from time to time.

"**Master**" refers to the individual(s) nominated by the Customer via an Online Enterprise Banking Services Application / Maintenance Form (and/or any other form and/or materials as required by the Bank from time to time) and approved by the Bank to do all the things as described at Clause 12.21(a), which may be amended from time to time.

"**Mobile Banking App**" means the "CCB (Asia) Business Mobile App", or such mobile banking application or software(s) as may be designated by the Bank from time to time made available from the App Store(s) for the purposes of accessing the Online Enterprise Banking Services (the features of which we may vary from time to time).

"**Mobile Device**" means, for the purpose of accessing and using any Online Enterprise Banking Services, a telephone or other device with access to a cellular radio system that allows users to make and receive telephone calls, text messages and utilise data services among other features, that can be used over a wide area without a physical connection to a network, such as a mobile smartphone, tablet computer, or similar device.

"**Mobile Token**" has the meaning as defined in the *Terms and Conditions for Mobile Token and Biometric Credential Authentication Service*.

"**Mobile Token Password**" has the meaning as defined in the *Terms and Conditions for Mobile Token and Biometric Credential Authentication Service*.

"**Online Enterprise Banking Services**" means the banking products or services which the Bank enables a Customer to access via the Mobile Banking App or the Website, and the relevant inbuilt features therein (including the Mobile Token and/or the Biometric Credential Authentication Service), as may be amended from time to time.

"**Online Enterprise Banking Services Application / Maintenance Form**" means any one of the application / maintenance forms submitted by the Customer to the Bank in a form prescribed by the Bank from time to time, for the purpose of applying for and/or amending access to the Online Enterprise Banking Services. The Customer must set out the individual(s) it designates as its Authorised Representative(s), who have the authority to act on its behalf via the Online Enterprise Banking Services.

"**Password**" means any confidential password, phrase, code or number or any other identification whether issued to the Customer by the Bank or adopted by the Customer (including any Security Code or (if applicable) any Mobile Token Password) which is used to access the Online Enterprise Banking Services.

"**PDPO Notice**" means the Notice to Customers relating to the Personal Data (Privacy) Ordinance of the Bank as may be amended from time to time.

"**Privacy Policy**" means the Personal Information Collection and Privacy Policy Statement of the Bank as may be amended from time to time.

"**Regulatory Requirement**" means any law, regulation or court order, or any rule, direction, guideline, code, notice or restriction (whether or not having the force of law) issued by any regulatory authority, governmental agency (including tax authority), clearing or settlement bank or exchange, or industry or self-regulatory body, whether in or outside Hong Kong, to which the Bank or its affiliates or group companies, or the Customer are subject or are expected to comply with from time to time.

"**Security Code**" means the one-time Password generated or displayed by the Security Device or the Mobile Token (as applicable) for use by the Authorised Representative to access the Online Enterprise Banking Services.

"**Security Device**" means an electronic device in physical form designated and provided by the Bank (upon request) for use by each Authorised Representative to generate the Security Code to access the Online Enterprise Banking Services.

"**Transaction Limit**" means any limit on any Online Enterprise Banking Services imposed by the Bank from time to time generally or upon any specific Customer, or subject to this foregoing limit, any limit on any Online Enterprise Banking Services imposed by the Customer in an Online Enterprise Banking Services Application / Maintenance Form from time to time. In respect of the limit imposed by the Bank, the Bank may add or remove any limits and/or vary the amount of any limit at any time.

"**User Guide**" means the guidelines which specify how the Online Enterprise Banking Services should be utilised by the Customer, as the same may be updated and amended from time to time.

"**User Name**" means the user short name used by an Authorised Representative, that is either a Master, an Authoriser or a Maker (as the case may be) to access the Online Enterprise Banking Services. Once such a User Name has been nominated by the Authorised Representative, such User Name cannot be changed.

"**Website**" means www.asia.ccb.com, http://hk.ccb.com/ or any other website which the Bank may advise the Customer of from time to time.

Use and updates

12.5 The terms of these Terms apply to the Mobile Banking App, the Website and the Online Enterprise Banking Services, including any updates or supplements to the Mobile Banking App, the Website or the Online Enterprise Banking Services, unless the Bank specifies that they are governed by separate terms and conditions, in which case those terms and conditions would apply. If any open-source software is included in the Mobile Banking App, the Website or the Online Enterprise Banking Services, the terms of an open-source licence may override some of the provisions of these Terms. The Bank may change these Terms at any time by notifying the Customer of such changes when the Customer next accesses to the Mobile Banking App or the Website. The new terms may be displayed on-screen and the Customer may be required to read and accept them to continue its use of the Mobile Banking App, the Website and the Online Enterprise Banking Services.

12.6 From time to time, there may be updates to the Mobile Banking App implemented through the App Store and/or updates to the Website. Depending on the settings of such updates, the Customer may not be able to use the Mobile Banking App, the Website and the Online Enterprise Banking Services until the Customer has downloaded the latest version of the Mobile Banking App or updated the browser (as the case may be) and accepted the new or additional terms and conditions (if any).

12.7 The Online Enterprise Banking Services (save for information provided by our licensors or by third-party service providers, such as market information and property valuation) are developed and solely owned by us. Any of the Online Enterprise Banking Services may be withdrawn, amended, suspended or terminated by the Bank at any time without prior notice. The Bank may at its absolute discretion decide whether the Customer or any of its Authorised Representatives is eligible to use any of the Online Enterprise Banking Services, and suspend its use of the Online Enterprise Banking Services, the Website and/or Mobile Banking App (or any part of them), or suspend its access (including, via the Mobile Token and/or the Biometric Credential Authentication Service) to the Online Enterprise Banking Services, the Website and/or Mobile Banking App without prior notice. The decision of the Bank is final. The Bank will not be responsible for any loss or damage suffered by the Customer arising from such decisions.

12.8 The Customer acknowledges that the Mobile Banking App and the Website have not been developed to meet its individual needs and requirements, and that it is therefore the Customer's responsibility to ensure that the facilities and functions of the Mobile Banking App or the Website meet its needs and requirements.

12.9 Subject to Clause 12.65, the Bank does not charge any fee for the use of the Mobile Banking App nor the Website. However, the Customer will be responsible for the charges associated with using the data service on its Mobile Devices or any other electronic devices. The Customer should check with its network operator for details of the usage fees.

The Mobile Banking App

12.10 The Customer will be assumed to have obtained permission from the owners of the Mobile Devices (e.g. mobile telephone or other handheld devices) that are controlled, but not owned, by the Customer and to download the Mobile Banking App onto the Mobile Devices. The Customer accepts full responsibility in accordance with the terms of these Terms for the use of the Mobile Banking App or the Online Enterprise Banking Services on or in relation to any Mobile Devices, whether or not such Mobile Devices are owned by the Customer.

12.11 The Mobile Banking App may only be used on compatible devices as specified by the Bank from time to time. The Bank does not guarantee that any specific device or model will be compatible with the Mobile Banking App. The Customer acknowledges that it is solely responsible for ensuring its Mobile Device meets the minimum requirements and it shall only download the Mobile Banking App and its updates from the official App Store. Failure to do so may result in the malfunctioning of the Mobile Banking App.

12.12 The Mobile Banking App will not run on any Mobile Devices which are compromised (e.g. "jailbroken"). The Bank shall not be responsible for any loss or damages suffered by the Customer in connection with the Customer's attempts to use the Mobile Banking App on such Mobile Devices.

The Online Enterprise Banking Services

12.13 Without prejudice and in addition to Clause 12.58 below, the Bank is, in its absolute discretion, entitled to determine and update or modify from time to time the extent and type of the Online Enterprise Banking Services available to the Customer at any time including, without limitation:

(a) expanding, modifying or reducing the Online Enterprise Banking Services;

(b) imposing and varying any restrictions (including, without limitation, Transaction Limit) applicable to the use of the Online Enterprise Banking Services; and

(c) prescribing and changing the normal service hours during which the Online Enterprise Banking Services are available and any daily cut-off time for any type of Online Enterprise Banking Services or transactions. The Customer's Instruction given to the Bank via the Mobile Banking App and/or the Website after any applicable daily cut-off time shall be deemed to be received on the next immediate business day. The Bank may determine business day and daily cut-off time by reference to the operating time of various markets in different time-zones.

12.14 None of the Online Enterprise Banking Services shall be deemed to constitute professional advice to be relied upon by the Customer. Where necessary, persons accessing or viewing the Mobile Banking App and/or the Website for the use of any of the Online Enterprise Banking Services should seek independent professional advice.

12.15 The Mobile Banking App and the Website provide a broad range of general information relating to rates, indexes and stock prices. The Customer acknowledges that such information has not been investigated, verified, monitored or endorsed by the Bank. The Bank does not warrant the accuracy, reliability, timeliness, completeness or correct sequencing of the information nor bear any legal liability for loss arising from any inaccuracy, omissions or incompleteness of the information, regardless of whether the information is provided by the Bank or a third party. The Customer acknowledges that some of the Online Enterprise Banking Services are provided by the Bank's licensors and/or third-party information providers. The Customer's use of such Online Enterprise Banking Services will require its agreement to certain additional terms and conditions provided by the applicable licensors and/or third-party information providers.

12.16 The Bank may make available general financial, market or other information and data ("**Market Information**") supplied by any person ("**Information Provider**") to the Customer via the Online

Enterprise Banking Services and may provide the Customer with reports compiled from the Market Information in any form, medium or means ("**Reports**"). The Market Information and the Reports are made available for reference only and are not intended for trading or other purposes. Neither the Bank nor any Information Provider shall be considered an investment adviser to the Customer or the Authorised Representative. Neither the Bank nor any Information Provider warrants, represents or undertakes the sequence, accuracy, truth, reliability, adequacy, timeliness or completeness of any of the Market Information or the Reports or whether it is fit for any purpose. Nor does either of the Bank or any Information Provider assume any liability (whether in tort or contract or otherwise) for any reliance on the Market Information or the Reports by the Customer, the Authorised Representative(s) or any other person. Specifically, the Bank is not responsible for any information provided by the third-party information providers in the Mobile Banking App or the Website and does not accept any liability for the provision of any unlawful, threatening, abusive, defamatory, obscene or indecent information or any type of material which violates or infringes third-party rights by such third parties.

12.17 It is the Bank's policy to maintain the availability of the Online Enterprise Banking Services for use at all times. However, some functionalities of the Online Enterprise Banking Services may not be available outside of normal service hours and the Customer will be notified of these service outages on the Mobile Banking App or the Website (as the case may be). The Bank may also suspend the Online Enterprise Banking Services (including Mobile Token or the Biometric Credential Authentication Service), including but without limitation where it suspects that there have been any security breaches, for routine or emergency maintenance checks or where the Bank is required to do so in compliance with Regulatory Requirements. The Bank will endeavour to notify the Customer on the Mobile Banking App or the Website (as the case may be) prior to any such service interruption or suspension, unless where it is not practicable or unlawful to provide such prior notice.

12.18 From time to time, the Bank may advertise its own products or services or those of other companies on the Mobile Banking App or the Website through which the Customer and its Authorised Representative(s) access the Online Enterprise Banking Services. If the Customer has requested the Bank not to send any marketing materials to them, such Customer's request will not apply to the advertisements posted on the Mobile Banking App nor the Website and the Customer consents to receiving these advertisements posted on the Mobile Banking App or the Website.

Marketing functions on the Mobile Banking App

12.19 Without limiting Clause 12.18, the Bank will send the Customer push notifications via the Mobile Banking App regarding general market information, promotional offers or other communications from the Bank. The Customer can turn off this functionality at any time by turning off the push notifications services on its Mobile Devices. The Bank will seek prior consent from the Customer before the sending of push notifications. The Customer may withdraw this consent at any time by turning off the push notification services on its Mobile Devices.

12.20 The social media sharing function in the Mobile Banking App will enable the Customer to share and repost certain information obtained from the Mobile Banking App on the Customer's accounts on various social media platforms (as designated by the Bank from time to time). This functionality will remain disabled so long as the Customer refrains from clicking on the "sharing" button in respect of any or all of the permitted social media accounts on its Mobile Device. As different Mobile Devices and social media platforms may offer different means to disable the social media sharing function, the Customer should check the settings of its Mobile Devices and its respective social media account for more information. By using the social media sharing function, the Customer acknowledges and accepts that the Customer is solely responsible for any content the Customer shares and reposts via its social media accounts, as well as the comments and remarks the Customer makes in connection therewith. Without limiting Clauses 12.61 to 12.64 below, the Bank will not be liable for any losses suffered by the Customer in connection with its use of the social media sharing function. The Customer further agrees and undertakes to forthwith remove any such content, comments and/or remarks disseminated via its social media accounts using the social media sharing function in the Mobile Banking App upon the request of the Bank in circumstances where the Bank reasonably determines that any such content, comments and/or remarks may be unlawful, inaccurate, misleading, inappropriate or prejudicial to the interests of the Bank in any respect. Currently, the social media sharing function in the Mobile Banking App can only be accessed in restricted mode and on designated mobile devices, the Bank will roll out the full version of the social media sharing function gradually.

Appointment of Authorised Representative(s)

12.21 The Customer shall, through its Authorised Representative(s), access the Online Enterprise Banking Services through the Mobile Banking App and/or the Website. The Customer shall be responsible for, by filling an Online Enterprise Banking Services Application / Maintenance Form or any other form as required by the Bank from time to time, nominating and authorising individual(s) to act as its Authorised Representative(s) in relation to the Online Enterprise Banking Services. All Authorised Representatives must comply with these Terms and the Existing Terms, as well as the Bank's other requirements (including, but without limitation to the requirements on customer identification) as may be imposed from time to time. Each Authorised Representative shall be assigned by the Customer with a specific authority level as categorised below:

(a) **Master:** where an Authorised Representative is designated as a Master, such a Master will be able to view and authorise transactions through the Online Enterprise Banking Services after (i) the Maker(s) have inputted/ prepared/ initiated the relevant transaction(s) and/or (ii) the Authoriser(s) have authorised the relevant transaction(s) through Online Enterprise Banking Services.

The Master may add, delegate and authorise such other individual(s) as Maker(s), modify or remove Maker(s) and also modify the non-transaction related contact details of Master(s), Authoriser(s) and Maker(s) via the Mobile Banking App or the Website (as the case may be). The Master can also assign the level of access for Authorisers and/or Makers and/or change the Transaction Limit (including the Transaction Limit for Authorisers and/or Makers) for and on behalf of the Customer. Where there are more than one Master nominated by the Customer, the Customer must specify in an Online Enterprise Banking Services Application / Maintenance Form (or any other form as required by the Bank) whether the relevant Master shall have the authority to act alone or must act jointly with a second Master;

(b) **Authoriser:** where an Authorised Representative is designated as an Authoriser, such an Authoriser will be able to view and authorise transactions after the Maker(s) has inputted /prepared /initiated the relevant transaction(s) through Online Enterprise Banking Services, subject always to the Transaction Limit applicable to such Authoriser assigned to it by the Master or the Customer from time to time.

(c) **Maker:** where an individual is designated as a Maker, such Maker will be able to view, input, prepare and initiate transactions through the Online Enterprise Banking Services, subject always to the Transaction Limit applicable to such Authoriser assigned to it by the Master or the Customer from time to time.

The assignment of these specific authority levels is subject to approval by the Bank. Any individual(s) designated as a Master or Authoriser must also be an authorised signatory for such Account(s) linked to Online Enterprise Banking Services. Where a Customer has applied for all its Accounts to be linked to the Online Enterprise Banking Services, it must ensure that all Masters and Authorisers are authorised signatories for each of such Accounts and all necessary corporate approvals of the Customer have been put in place and provided in such form(s) as required by the Bank. All Authorised Representatives will be subject to the Transaction Limit imposed on the Customer for the relevant Account(s).

For the avoidance of doubt, the specific authority level designated to an Authorised Representative under the Online Enterprise Banking Services shall only apply to the Customer's use of the Online Enterprise Banking Services, and will not extend beyond this to any other services, products provided by the Bank or any other transactions to be entered into by such Customer with the Bank.

12.22 If the Customer has more than one Authorised Representative, each of the Authorised Representatives will be assigned a unique User Name and Customer Number. The Bank will provide the respective sets of User Name and Customer Number to the Customer, who shall be responsible for delivering the respective sets of User Name and Customer Number to each of the nominated Master(s), Authoriser(s) and/or Maker(s).

Instructions to the Bank

12.23 For the purpose of the Online Enterprise Banking Services, the Bank shall be entitled (but not bound) to accept and rely on any or all Instructions provided to it by the Customer through the Mobile Banking App and/or the Website, and the Customer shall be responsible for and be bound by all such Instructions regardless of whether such Instructions are given by the Customer or their Authorised Representatives.

12.24 The Bank will receive and act on Instructions with respect to the Customer's Account(s) or other relationships or matters with the Bank, subject always to the following:

(a) the Bank shall ensure that before carrying out any Instruction, the Instruction is authenticated by the Bank through checking any one or more of the Customer's User Name, Customer Number, Password, Security Code, (if applicable) Mobile Token Password under the Mobile Token and (if applicable) Biometric Credentials under the Biometric Credential Authentication Service (collectively, "**Identity Verification Information**"), but without the obligation to carry out any further inquiry, authentication or other steps as to the authority of person who submitted the Instruction;

(b) the Bank shall be entitled (but not obliged) to give effect to any Instruction received, on such terms as received. The Bank's record of any Instruction shall be final and binding (unless there is a manifest error);

(c) the Bank may refuse to act on any Instruction at its absolute discretion, including if, in the Bank's opinion:

(i) it is not practicable or reasonable for the Bank to do so, or that it is not in accordance with its regular business practices and procedures;

(ii) the Instruction exceeds the applicable Transaction Limit;

(iii) the Bank knows or suspects that there has been a breach of security in relation to the Customer's Account(s) or the Online Enterprise Banking Services; or

(iv) the Online Enterprise Banking Services has been terminated.

(d) the Bank reserves the right to restrict the number and/or type of Mobile Devices and/or any other electronic devices which may be registered by the Customer for accessing the Online Enterprise Banking Services from time to time;

(e) the Bank accepts no responsibility for the accuracy or completeness of any data, or corruption, interception, deletion or loss of data due to any fault, failure or malfunctioning of the Customer's Mobile Devices and/or any other electronic devices;

(f) the Customer will be bound by any Instruction;

(g) the Customer will be responsible for ensuring that the Instructions provided to the Bank via the Online Enterprise Banking Services are accurate and complete;

(h) the Customer will check all bank statements and notifications from the Bank promptly and notify the Bank of any errors or unauthorised transactions; and

(i) despite an electronic acknowledgement may be issued once the Bank receives an Instruction, under certain circumstances, an Instruction may not actually be processed until the next processing day for Instructions of that kind.

12.25 Once given, an Instruction may not be amended, cancelled or withdrawn. All Instructions (as received and acted on by the Bank in good faith) shall be irrevocable and binding on the Customer whether given by the Customer or by any other person. The Bank shall have no obligation or duty to enquire or verify the authenticity of any Instruction or the identity or authority of any person giving any Instruction, other than to verify any one of the Identity Verification Information and the Bank shall not be liable to any party in any manner whatsoever.

12.26 The Customer agrees and acknowledges that where it provides to the Bank an Instruction through the Online Enterprise Banking Services, such an Instruction shall not be deemed to have been executed until the Customer receives a confirmation from the Bank on its completion. Certain types of Instructions may not be processed outside of normal service hours, and there may be a delay in its execution. In circumstances where the placing of certain types of Instructions requires the Customer's provision of additional supporting documents, the relevant Instruction will not be processed until the Bank has received all of the requested supporting documents in such form and substance to the satisfaction of the Bank.

12.27 In additional to the Instruction submitted by the Customer on the Mobile Banking App or the Website (as the case may be), the Customer hereby authorises the Bank, from time to time, to act upon written instructions or requests it receives from the Customer, in relation to the Online Enterprise Banking Services, where such written instructions or requests are in the form of a board resolution from the

Customer, or any authorised person who has been authorised by the board of directors of the Customer to act on its behalf to provide instructions to the Bank for this purpose. Such written instructions or requests may include, without limitation to, the following:

(a) adding, removing or replacing any Authorised Representative(s);

(b) resetting any Password, for whatever reason; or

(c) any action in relation to the access to or use of the Online Enterprise Banking Services.

Security measures

12.28 Access to the Online Enterprise Banking Services may require the use of valid Identity Verification Information.

12.29 The Customer acknowledges and accepts that any person who gains access to or acquires knowledge of the Customer's Identity Verification Information will be able to access the Online Enterprise Banking Services and give Instructions to the Bank in respect of the Customer's account(s) maintained with the Bank, including but not limited to placing orders, withdrawing or otherwise dealing with the Customer's funds. The Customer must take appropriate measures to safeguard the Identity Verification Information, which include, without limitation, the following:

(a) changing its Password or Mobile Token Password (where applicable) on a regular basis and refraining from disclosing its Password or Mobile Token Password (where applicable) to any person who is not authorised to have access to the Password or the Mobile Token Password (where applicable), including any member or officer of the Bank;

(b) refraining from selecting any Password or any Mobile Token Password (where applicable) which has been used before, or which is likely to be guessed by anyone attempting to access the Online Enterprise Banking Services. For example, an Authorised Representative should not choose a birthday or telephone number as a Password or a Mobile Token Password (where applicable);

(c) destroying any correspondence from the Bank concerning the Password as soon as possible;

(d) informing the Bank immediately if the Customer or any Authorised Representative is aware of or suspects that anyone has access to its Password, Mobile Token Password (where applicable), Security Code, Mobile Token or Security Device. The Online Enterprise Banking Services will be suspended immediately until a new Password or a new Mobile Token Password (where applicable) has been set up;

(e) changing the Password and the Mobile Token Password (if applicable) immediately if the Customer suspects that it has been deceived by any fraudulent website, mobile application, email or SMS/WAP push message (for example, if the Customer fails to log on to the Mobile Banking App after using the correct Biometric Credentials, with or without any alert messages);

(f) never leaving a device or Mobile Device unattended, once the Customer has logged onto the Online Enterprise Banking Services nor allow others to use the Mobile Device and/ or any other electronic device until the Customer has logged out of the Online Enterprise Banking Services;

(g) refraining from logging in to the Online Enterprise Banking Services on device or Mobile Device connected to a local area network or public terminal, without ensuring that no third parties can observe or copy a Customer's access. This includes being vigilant while logging into the Online Enterprise Banking Services via the Mobile Device and/or any other electronic device available at any of the Bank's branches or any other public areas;

(h) informing the Bank if any Authorised Representative leaves its employment, and revoking its mandate to act on behalf of the Customer. The Customer must ensure that these individuals do not have access to the Online Enterprise Banking Services;

(i) ensuring that the computer system, Mobile Device and/ or any other electronic device used for accessing the Online Enterprise Banking Service has the latest security patches and that all reasonably practicable measures are taken to ensure that any device used to access the Online Enterprise Banking Service is free from any computer virus or other such malware;

(j) informing the Bank immediately if a Security Device or a Mobile Token is not working, or there

are any problems with logging onto the Online Enterprise Banking Services; and

(k) referring to and complying with all other security safeguards as set out and updated from time to time on the Website, the Mobile Banking App and in the User Guide.

The Customer may be held liable for the losses if it has failed to comply with any of the above safeguards.

12.30 The Customer agrees to hold the Bank, its affiliates and/or its licensees (as applicable) fully indemnified against all losses, damages, costs and expenses (including professional and legal costs) if any person other than the Customer gains access to or acquires knowledge of the Customer's Identity Verification Information. The Bank will not be responsible for any losses arising out of any unauthorised transactions except due to any causes set out in Clause 12.61.

12.31 The Bank may, in its sole discretion, require the Customer to use a Security Code to access the Online Enterprise Banking Services or give certain types of Instructions. It is the sole responsibility of the Customer to make a request for a Security Device or to set up a Mobile Token.

12.32 The Security Device or Mobile Token (where applicable) shall remain the property of the Bank and shall (in the case of the Security Token) be immediately returned to the Bank or disposed of in accordance with the Bank's instructions or (in the case of the Mobile Token) be deregistered or otherwise disabled immediately upon termination of the Online Enterprise Banking Services.

12.33 The Customer shall use the Security Device or the Mobile Token (where applicable) in a proper manner. The Customer shall not change, tamper or modify the Security Device nor interfere with, manipulate, damage, disrupt or reverse-engineer the Mobile Token (where applicable) without the Bank's prior written consent or cause any loss or damage to the Security Device and the Mobile Token (where applicable). The Customer shall notify the Bank as soon as reasonably practicable after becoming aware of any loss, damage, corruption, compromise, unauthorised use or failure of the Security Device and/or the Mobile Token. The Bank shall not be liable for any loss incurred by the Customer in connection with any loss, damage, corruption, compromise, failure, defect, malfunctioning or breakdown of the Security Device, the Mobile Device or the Mobile Token.

Mobile Token and Biometric Credential Authentication Service

12.34 Further terms and conditions of services in relation to the accessing of the Mobile Banking App via the Mobile Token and/or the Biometric Credential Authentication Service are set out in the *Terms and Conditions for Mobile Token and Biometric Credential Authentication Service*.

Data collection

12.35 In providing the Online Enterprise Banking Services, the Bank, its affiliates and/or its licensees (as applicable) may collect personal data relating to the Authorised Representatives and/or any directors, officers, employees, authorised persons of the Customer (collectively, "**Relevant Persons**") for various purposes, including but not limited to facilitating the Bank's provision of the Online Enterprise Banking Services and promotion of the Bank's other products and services. The collection, use, transfer, processing, retention, maintenance and handling of any such personal data by the Bank, its affiliates and/or its licensees, are subject to the Bank's Privacy Policy and PDPO Notice. The Customer acknowledges that it has read the terms of the Privacy Policy and PDPO Notice and confirms that it will obtain and/or has obtained the consent from the Relevant Persons regarding the use of their personal data by the Bank and/or its affiliates and licensees.

12.36 By using the Mobile Banking App, the Website, the Mobile Token or any of the Online Enterprise Banking Services, the Customer consents to the Bank, its affiliates and/or its licensees' collecting and using the location of its Mobile Devices and/or any other electronic device and technical information such as IP address, advertising ID, unique device identifier, and device type, information about the operating system and application software used on its Mobile Device and/or any other electronic device and other non-personal information, related software, hardware and peripherals for the Online Enterprise Banking Services in the Mobile Token, the Mobile Banking App or the Website that are internet-based or wireless to facilitate the Bank, its affiliates and/or its licensees in improving its products and services to the Customer.

12.37 The Customer acknowledges and agrees that the Bank, its affiliates and/or its licensees may track and record the Customer's browsing activities on the Mobile Banking App or the Website. The Bank, its affiliates and/or its licensees will use the aggregated information, including user demographics

and behaviour and usage patterns, to enhance reporting accuracy and the effectiveness of marketing. No personal data or personally identifiable information of the Customer will be stored in the Mobile Banking App nor the Website. The Bank will use reasonable endeavours to take practical steps (or will use reasonable endeavours to procure its affiliates and/or licensees) to ensure that the information collected will not be kept longer than necessary and that the Bank, its affiliates and/or its licensees will comply with all Regulatory Requirements applicable to the retention of information collected.

12.38 For technical reasons, it may be not possible for the Customer to opt out of the online behavioural tracking in the Mobile Banking App nor the Website. The Customer should stop using the Mobile Banking App or the Website if the Customer does not consent to the collection and use of its personal data or other information by the Bank, its affiliates and/or licensees.

12.39 Unless otherwise set out in these Terms, the Bank, its affiliates and/or licensees will not:

(a) transfer the Customer's usage behavioural information collected from the Mobile Banking App nor the Website to any third party;

(b) work with any third party to record the Relevant Persons' personal data; and

(c) combine the usage data collected from the Mobile Banking App nor the Website with other information collected from other sources or channels to track or profile the Customer.

12.40 The Mobile Banking App or the Website will collect data and information regarding the Customer's location, or the location of its Mobile Devices and/or any other electronic device, by using GPS coordinates sent from its Mobile Devices and/or any other electronic device. The GPS coordinates are collectively referred to as "location data". The Customer's use of the map function is subject to and conditional upon its agreement to Google Map's Terms of Use (https://www.google.com/intl/en-US/help/terms_maps.html). The Customer may turn off this functionality at any time by turning off the location services settings on its Mobile Devices and/or any other electronic device. The Bank, its affiliates and/or its licensees will seek the Customer's consent before the Bank, its affiliates and/or licensees transmit, collect, retain, maintain, process and use the Customer's location data and queries to provide and improve location-based and road traffic-based products and services. The Customer may withdraw this consent at any time by turning off the location services settings on its Mobile Devices and/or any other electronic device.

12.41 The collection and use of the Customer's personal data and other information are for analytical and marketing purposes to enhance customer experience and improve marketing effectiveness. The Customer acknowledges that:

(a) such information will enable the Bank, its affiliates and/or its licensees to develop more useful features for the Customer, tailor the content of the Mobile Banking App and the Website to suit the Customer's needs and, to the extent permitted by the marketing preferences determined by the Customer, provides the Customer with promotional materials or direct marketing based on its usage patterns; and

(b) by configuring its preferences or options in its Mobile Devices, the Customer may determine to opt out or limit personalisation of advertisement preferences and turn off the location services settings.

12.42 The Customer further acknowledges and consents that its personal data and information will be collected, stored, accessed, used and handled for the purposes described in Clause 12.41. The Customer further acknowledges that, should it decide to withdraw its consent to such personal data or information collection, the Customer may change the settings on its Mobile Devices and/or any other electronic device. The Customer understands that as a result of the withdrawal of its consent, it may not be able to use certain function(s) of the Mobile Banking App and/or the Website.

12.43 The Bank, its affiliates and/or its licensees may also work with third-party research agencies to research on certain usage and activities on the Mobile Banking App and the Website. Such third-party research agencies may use technologies such as advertising ID tracking to conduct research on user behaviour, usage patterns or other similar information for marketing research to improve the effectiveness of the Bank, its affiliates and/or licensees' marketing activities. Information collected from the Mobile Banking App and/or the Website will be aggregated and shared with the Bank, its affiliates and/or its licensees. No personally identifiable information in relation to the Customer or the Relevant Persons will be collected or shared by such third-party research agencies with the Bank, its affiliates and/or licensees as a result of the aforementioned research. The Customer acknowledges

and agrees that, should it decide to disable its advertising ID, the Customer may change the settings on its the Mobile Devices and/or any other electronic device.

Licence

12.44 The Bank grants the Customer a non-transferable, non-sublicensable and non-exclusive licence to use the Mobile Banking App and the Website on its Mobile Devices and/or any other electronic device in order to access the Online Enterprise Banking Services, subject to the provisions of:

(a) these Terms;

(b) the Privacy Policy and the PDPO Notice;

(c) the App Store Rules; and

(d) the Existing Terms.

12.45 The Customer may download the Mobile Banking App onto its Mobile Devices and view, use and display the Mobile Banking App, the Website, and the Online Enterprise Banking Services on the Mobile Devices and/or any other electronic device solely for the domestic and personal use by the Customer and the Authorised Representatives.

12.46 The Customer agrees not to use the Mobile Banking App, the Website and the Online Enterprise Banking Services for any commercial, business or resale purposes.

The Customer's responsibilities

12.47 Except as expressly set out in these Terms or as permitted by any Regulatory Requirements, the Customer undertakes and warrants:

(a) not to use the Mobile Banking App, the Website and the Online Enterprise Banking Services (including the access via the Mobile Token and/or the Biometric Credential Authentication Service) in any way that breaches any applicable Regulatory Requirements, including all technology control or export laws and regulations that apply to the technology used or supported by the Mobile Banking App, the Website, the Mobile Token, the Biometric Credential Authentication Service or any Online Enterprise Banking Services ("**Technology**");

(b) not to copy the Mobile Banking App, the Website or the Online Enterprise Banking Services for any purposes;

(c) not to rent, lease, sub-license, loan, translate, merge, adapt, vary or modify the Mobile Banking App, the Website or the Online Enterprise Banking Services;

(d) not to make alterations to, or modifications of, the whole or any part of the Mobile Banking App or the Website or permit the Mobile Banking App, the Website or any part of it to be combined with, or become incorporated in, any other programs;

(e) not to disassemble, decompile, reverse-engineer or create derivative works based on the whole or any part of the Mobile Banking App or the Website;

(f) not to sell, vary, display, modify, reproduce, stored in a retrieval system, transmit, copy or distribute (in any form or by any means), or use as materials for creative work or otherwise use in other commercial or public purposes without the prior written consent from the Bank or its licensors;

(g) not to provide or otherwise make available the Mobile Banking App or the Website in whole or in part (including object and source code), in any form to any person without prior written consent from the Bank;

(h) not to use the Mobile Banking App, the Website, the Mobile Token, the Biometric Credential Authentication Service or the Online Enterprise Banking Services in any unlawful manner, for any unlawful purpose, or in any manner inconsistent with these Terms, or act fraudulently or maliciously, including but without limitation to hacking into the Mobile Banking App, the Website or any operating system;

(i) not infringe the Bank's intellectual property rights or those of any third party in relation to its use of the Mobile Banking App, the Website, the Mobile Token, the Biometric Credential

Authentication Service or any Online Enterprise Banking Services (to the extent that such use is not licensed by these Terms);

(j) not transmit any material that is defamatory, offensive or otherwise objectionable in relation to its use of the Mobile Banking App, the Website or any Online Enterprise Banking Services;

(k) not to transmit any data, send or upload any material that contains viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar computer code designed to adversely affect the operation of the Mobile Banking App, the Website, the Mobile Token, the Biometric Credential Authentication Service, any Online Enterprise Banking Services or any operating system;

(l) not use the Mobile Banking App, the Website, the Mobile Token, the Biometric Credential Authentication Service or any Online Enterprise Banking Services in a way that could damage, disable, overburden, impair or compromise the Bank's systems or security or interfere with other users;

(m) not collect or harvest any information or data from the Mobile Banking App, the Website or the Bank's systems or attempt to decipher any transmissions to or from the servers running the Mobile Banking App or the Website;

(n) not to access without authority, interfere with, manipulate, damage or disrupt:

(i) any part of the Mobile Banking App nor the Website;

(ii) any device, Mobile Device or network on which the Mobile Banking App or the Website is stored;

(iii) the Mobile Token or any software used in the provision of the Mobile Banking App or the Website; or

(iv) any device, Mobile Device or network or software owned or used by any third party.

12.48 The Customer acknowledges and agrees that, as a condition of using the Online Enterprise Banking Services to give Instructions, the Customer will immediately notify the Bank if:

(a) an Instruction has been placed through the Online Enterprise Banking Services and the Customer has not received an Instruction number or has not received an accurate acknowledgement of the Instruction or of its execution (whether by hard copy, electronic or verbal means);

(b) the Customer has received acknowledgement (whether by hard copy, electronic or verbal means) of an Instruction which the Customer did not issue or has error or irregularity;

(c) the Customer becomes aware of any of the acts mentioned in Clause 12.47 being done or attempted by any person;

(d) the Customer becomes aware of any unauthorised and/or illegal use of the Identity Verification Information belonging to itself; or

(e) the Customer has difficulties in the use of the Online Enterprise Banking Services.

If the Customer fails to report such incidents to the Bank as soon as reasonably practicable, or has otherwise acted fraudulently or with gross negligence, the Customer may be held responsible for all such transactions and all direct losses as a result.

12.49 The Customer acknowledges that the Online Enterprise Banking Services, the Website, the Mobile Banking App, the Mobile Token and the software comprised in them, are proprietary to the Bank. Where the Bank has reasonable ground to suspect that the Customer has breached any of its warranties and undertakings in these Terms (including Clause 12.47), the Customer agrees that the Bank shall be entitled to close any or all of the account(s) maintained by the Customer with the Bank immediately without notice to the Customer and take legal action against the Customer. The Customer undertakes to notify the Bank immediately if the Customer becomes aware that any of the actions described above in Clause 12.47 is being perpetrated by any other person.

12.50 The Customer acknowledges that the communication facilities adopted by the Bank (including the Internet) for the purpose of the transmission or communication of instructions or any information through the Online Enterprise Banking Services (including the access via the Mobile Token and/or the Biometric Credential Authentication Service), the Website and the Mobile Banking App may be

unreliable or unavailable at any time, causing interruption, delay, corruption or loss of data, the loss of confidentiality in the transmission of data, or the transmission of malware may occur when transmitting data via such communication facilities. Also, transmission or communication of instructions or any information through the Online Enterprise Banking Services, the Website and the Mobile Banking App between the Customer and the Bank may be delayed as a result of a range of factors, including but without limitation to time zone differences, public holidays in Hong Kong SAR or overseas, or other reasons beyond the control of the Bank, and the Bank should not be liable for such delay or any interest thereon (if any). The Customer accepts all risks arising from its acceptance of any of the Online Enterprise Banking Services (including the access via the Mobile Token and/or the Biometric Credential Authentication Service) made available by the Bank, including but not limited to, any loss suffered as a result of any delay, error or omission of transmission and communication of instructions or any information through the Online Enterprise Banking Services between the Customer and the Bank.

12.51 The Customer acknowledges that no representation or warranty is given by the Bank as to the timeliness, sequence, accuracy or completeness of market data or any market information provided to the Customer through Online Enterprise Banking Services, the Website and the Mobile Banking App.

12.52 The Customer's use of the Mobile Banking App, the Website, the Mobile Token and the Online Enterprise Banking Services is wholly at its own risk. The Mobile Banking App, the Website, the Mobile Token and the Online Enterprise Banking Services are provided on an "as is" basis. To the fullest extent permitted by the Regulatory Requirements, the Bank disclaims all conditions, warranties (including, but not limited to, any warranties of merchantability, fitness for a particular purposes, accuracy and non-infringement of third party rights), representations or other terms which may apply to the Mobile Banking App, the Website, the Mobile Token and the Online Enterprise Banking Services, whether express or implied.

12.53 The Customer acknowledges that the Bank is not responsible for the content available on or the set-up of any other websites or resources linked to the Bank's Mobile Banking App and the Website. Access to, and use of, such other websites or resources is entirely at the Customer's own risk and subject to any terms and conditions that may be applicable to such access or use. Any website hyperlinked on the Bank's Mobile Banking App or the Website is for reference only. The Bank shall not be deemed to control, endorse, recommend, approve, guarantee or introduce any third parties or any of the services or products that they provide on their websites, whether directly or indirectly, nor does the Bank have any form of cooperation with such third parties and websites.

12.54 The Bank makes no representations or warranties as to the accuracy, functionality or performance of any third party software used in connection with the Mobile Banking App and the Website, or the compatibility of any particular Mobile Device and/or any other electronic device with the Mobile Banking App or the Website. The Customer are solely responsible for ensuring that its devices or Mobile Devices meet the specified system requirements.

12.55 Any exchange rate, interest rate, dealing rate and other prices and information quoted by the Bank on the Mobile Banking App, the Website or otherwise in response to an online inquiry is for reference only and is not binding on the Bank. Any interest rate, exchange rate, price and information offered by the Bank for the purpose of the relevant transaction shall be binding on the Customer upon its acceptance irrespective of any different interest rate, exchange rate, price or information quoted by the Bank.

12.56 The Customer and its Authorised Representative(s) acknowledge that there may be a time lag in transmission of instructions, information or communication via the internet.

Intellectual property rights and information ownership

12.57 The Customer acknowledges that:

(a) all intellectual property rights (including but not limited to trade marks, logos and service marks) in the Mobile Banking App, the Website, the Mobile Token, the Online Enterprise Banking Services and the Technology anywhere in the world belong to the Bank or its licensors;

(b) the Mobile Banking App and the Website are licensed (and not sold) to the Customer for use only, as such the Customer has no rights in, or to, the Mobile Banking App, the Website, the Mobile Token, the Online Enterprise Banking Services or the Technology other than the right to use each of them in accordance with these Terms;

(c) the Customer has no right to have access to the Mobile Banking App or the Website in source-code form; and

(d) all information submitted to the Bank via the Mobile Banking App or the Website and all electronic records and documents in connection with any communication between the Bank and the Customer via the Mobile Banking App or the Website shall be deemed and remain the property of the Bank.

Service availability and termination

12.58 Subject to Regulatory Requirements, the Online Enterprise Banking Services (including its access via the Mobile Token and/or the Biometric Credential Authentication Service) may be suspended, terminated, withdrawn or amended by the Bank at any time without prior notice or providing any reason. Subject to Regulatory Requirement applicable to the Bank, the Bank is under no obligation to continuously provide the Online Enterprise Banking Services (including its access via the Mobile Token and/or the Biometric Credential Authentication Service). The Bank may, in its absolute discretion, suspend the Customer's use of the Online Enterprise Banking Services or any part of it, or suspend the Customer's access to the Online Enterprise Banking Services without prior notice as the Bank considers appropriate. The Bank's decision in this regard is final and binding on the Customer. The Bank will not be responsible for any loss or damage suffered by the Customer arising from such decisions.

12.59 Among others, the Customer may be restricted from accessing the Online Enterprise Banking Services if:

(a) the Customer does not activate the Online Enterprise Banking Services after 60 days from our notification or such other period as prescribed by the Bank;

(b) the Online Enterprise Banking Service is not accessed or used for a continuous period of 1 year; or

(c) it is determined by the Bank that the Customer is not eligible to use the Online Enterprise Banking Services.

The Customer may contact the Bank to apply for re-accessing Online Enterprise Banking Services.

12.60 Without limiting Clause 12.7, these Terms can be terminated by the Customer by giving prior notice to the Bank in the form and by means specified by the Bank from time to time. The Customer agrees that any notice of termination originated from the Customer will only become effective when the Bank confirms the termination. Any suspension or termination of the Online Enterprise Banking Services will not affect any of the rights or obligations which may have accrued on or before the date of suspension or termination, and the provisions of these Terms will continue to bind the Customer after the termination of these Terms to the extent that they relate to any obligations or liabilities of the Customer which remain to be performed or discharged.

The Bank's rights and limitation of liability

12.61 Subject to Clauses 12.62 and 12.63 below, the Bank will only be liable where the Customer has suffered direct losses from its use of the Online Enterprise Banking Services and such losses are attributable to the gross negligence, fraud or wilful misconduct of the Bank.

12.62 Without prejudice to Clause 12.58 above, the Bank reserves the right to vary, cancel, terminate or suspend the whole or any part of the Online Enterprise Banking Services without giving notice or reason. The Customer agrees that, to the fullest extent permissible under the Regulatory Requirement applicable to the Bank, in the absence of gross negligence, fraud or wilful misconduct, neither the Bank, nor any of its officers or employees shall be liable for any loss, damage, cost or expense of any kind which the Customer or any other person may incur or suffer in connection with the Bank's exercise of the above mentioned right.

12.63 In addition to Clause 12.62 above, the Bank will not be liable to the Customer for any loss or damages from the Customer's use of the Online Enterprise Banking Services in the instances including, without limitation:

(a) any interruption, delay, suspension, interception, loss or other failure in the Bank providing the Online Enterprise Banking Services (including its access via the Mobile Token and/or the Biometric Credential Authentication Service), in transmitting any Instructions or information via

the Online Enterprise Banking Services, which are beyond the reasonable control of the Bank, including, without limitation, failures of communication networks, systems, any act or omission of third party providers, breakdown of equipment or any government order;

(b) any Instruction originated by a third party without authorised access to the Online Enterprise Banking Services, the Website or the Mobile Banking App and subsequently acted upon by the Bank upon authentication of the Customer's Identity Verification Information;

(c) where the Customer fails to carry out any of the responsibilities under these Terms; and

(d) any loss of or damage to the Customer's data, software, computer, computer networks, telecommunications or other equipment caused by the Customer's use of the Online Enterprise Banking Services, unless such loss or damages is directly and solely caused by the Bank's gross negligence, fraud or wilful misconduct.

If the Bank is found liable for any act or omission whatsoever, the Bank's liability will be limited to the amount of the relevant transaction or direct damages (whichever is less). The Bank will not be liable for any indirect, special or consequential loss or damages.

12.64 To the fullest extent permitted by the Regulatory Requirements, the Customer agrees to indemnify the Bank, its employees or officers and to keep the Bank, its employees or officers indemnified against any claims, actions, proceedings, losses, damages or expenses whatsoever and howsoever caused, brought against the Bank, its employees or officers, except for any direct loss or damages caused by the negligence or fraud on the part of the Bank, its employees or officers, in relation to the provision of the Online Enterprise Banking Services. This includes, but is not limited to instances where the Bank, its employees or officers have acted on the Customer's Instructions, the Customer has improperly used the Online Enterprise Banking Services and the Customer has not complied with any provisions of these Terms.

Miscellaneous

12.65 The Customer agrees to pay all fees and charges (if any) associated with using the Online Enterprise Banking Services. These fees and charges are set out in full on the Mobile Banking App, the Website and, in addition to these fees (if any), the Bank may also charge fees for other products and services. The Customer authorises the Bank to deduct any fees from the Customer account(s) maintained with the Bank (where applicable) for using the Online Enterprise Banking Services.

12.66 These Terms may be amended at any time, or the Bank may introduce additional terms and conditions to these Terms from time to time. The amended Terms will become effective upon the Bank giving reasonable notice to the Customer, including posting the amended Terms on the Mobile Banking App, on the Website or displaying the amended Terms in the Bank's branches (where appropriate). By continuing to use the Online Enterprise Banking Services, subject to Regulatory Requirements, the Customer is deemed to have agreed to the amended Terms.

12.67 The Bank has a very high level of encryption and the use of such levels of encryption may be illegal in jurisdictions outside of Hong Kong. The Customer is responsible for ensuring, if they are outside Hong Kong, that the use of the Online Enterprise Banking Services is permitted by local law and the Bank will not be liable for any loss or damages suffered by the Customer as a result of its not being able to use the Online Enterprise Banking Services in such jurisdictions.

12.68 Any notice or communication to be made under these Terms shall be deemed to have been served or delivered if sent:

(a) by facsimile, when confirmed by an activity report confirming the facsimile number to which such notice was sent, the number of pages transmitted and that such transmission was successfully completed at the time of despatch;

(b) by hand, at the time left at the relevant address;

(c) by post to an address in Hong Kong, 48 hours after being put in the post with prepaid postage ad being properly addressed;

(d) by prepaid post, to an address outside Hong Kong, 7 Business Days following that on which it was so posted; or

(e) by electronic means, at the time of transmission if the message is sent by the Bank and, at the time the message is actually received by the Bank if the message is sent by the Customer.

12.69 If the whole or any part of any provision of these Terms is void, unenforceable or illegal in a jurisdiction, it is severed for that jurisdiction. The remainder of these Terms has full force and effect and the validity or enforceability of a provision in any other jurisdiction is not affected.

12.70 Supplementary terms may apply to Customers who use the Online Enterprise Banking Services in certain jurisdictions. For more details on these supplementary terms and to which jurisdictions these supplementary terms apply, the Customer should refer to the Mobile Bank App.

12.71 These Terms and the Online Enterprise Banking Services are governed by the laws of the Hong Kong Special Administrative Region. The Customer agrees to submit to the non-exclusive jurisdiction of the Hong Kong courts in relation to any dispute in respect of or arising from these Terms and the Online Enterprise Banking Services, but these Terms may be enforced in the courts of any competent jurisdiction.

12.72 In the event of any inconsistency between the English version and the Chinese version of these Terms, the English version of these Terms will prevail.

12.73 No person other than the Bank and the Customer will have any right under the Contracts (Rights of Third Parties) Ordinance ("**Third Party Ordinance**") to enforce or enjoy the benefit of any of the provisions of these Terms. Notwithstanding any provision contained herein, the consent of any person who is not a part to these Terms is not required to rescind or vary these Terms at any time. For the avoidance of doubt, any director, officer, employee, affiliate or agent of the Bank may, by virtue of the Third Party Ordinance, rely on any clause of these Terms which expressly confers rights or benefits on that person.

12.74 These Terms shall be binding upon, and enure to the benefit of, the parties to these Terms and their respective successors and permitted assigns.

12.75 The Customer shall not assign any of its rights, benefits, powers, obligations or liabilities under these Terms. The Bank may at any time assign all or any of its rights, benefits, powers, obligations or liabilities under these Terms to any other person without any consent from or any prior notification to the Customer.

Terms and Conditions for Mobile Token and Biometric Credential Authentication Service ("Annex 1")

This Annex 1 is the *Terms and Conditions for Mobile Token and Biometric Credential Authentication Service* referred to in clause 12.34 of the *Specific Terms and Conditions for Online Enterprise Banking Services*, as the same may be amended from time to time.

General

1. This Annex 1 applies to Customers who use (1) the Mobile Token and/or (2) the Biometric Credential Authentication Service (each as defined in Clause 3 in this Annex 1) made available by the Bank.

2. This Annex 1 is in addition and supplemental to the Specific Terms and Conditions for Online Enterprise Banking Services (the **"Terms**"). For the avoidance of doubt, in the event that there is any inconsistency between the provisions set out in this Annex 1 and the provisions set out in other parts of the Terms, this Annex 1 shall prevail in relation to the Mobile Token and the Biometric Credential Authentication Service.

3. Upon successful activation, the Customer will be allowed to use the biometric credentials (including, without limitation, fingerprint(s), facial map or any other biometric data) registered on the Customer's Permitted Mobile Device (defined below) to access the Online Enterprise Banking Services via the Mobile Banking App ("**Biometric Credential Authentication Service**"), including, without limitation, to use the mobile token feature in-built (if applicable) within the Mobile Banking App / Permitted Mobile Device for customer identity authentication purposes ("**Mobile Token**").

Definitions and interpretation

4. Words or phrases defined in the Terms shall have the same meanings as in this Annex 1 (save where otherwise expressly provided in this Annex 1).

5. For the purpose of this Annex 1,

   "**Permitted Mobile Device**" means any Mobile Device which the Bank may permit for use with the Mobile Token and/or Biometric Credential Authentication Service from time to time, including, without limitation, the operating system or software that the Mobile Device operates on.

   "Biometric Credentials" means biometric credentials including, without limitation, fingerprint, facial map or any other biometric data that is registered in the Customer's Permitted Mobile Device for the purpose of accessing the Online Enterprise Banking Services.

   "Mobile Token" means a feature in-built within and linked to the Mobile Banking App which is used to generate a Security Code or otherwise to authenticate and grant the Customer access to and/or use of any Online Enterprise Banking Services.

   "Mobile Token Password" means the personal identification number self-selected and designated by the Customer for the purpose of utilizing the Mobile Token.

6. Please visit https://www.asia.ccb.com/hongkong/doc/commercial/faq_oebs_mb.pdf for the current list of such Permitted Mobile Devices.

Eligibility

7. To use the Mobile Token and/or the Biometric Credential Authentication Service (if applicable), the Customer must have:

   (a) a valid Account with the Bank;

   (b) registered with Online Enterprise Banking Services;

(c) installed the Mobile Banking App where the Bank offers the Mobile Token and Biometric Credential Authentication Service and latest updates on the Customer's Permitted Mobile Device;

(d) (only applicable to Biometric Credential Authentication Service) a Permitted Mobile Device with the biometric authentication function enabled;

(e) (only applicable to Biometric Credential Authentication Service) registered at least one of the Customer's Biometric Credentials to control access to the Permitted Mobile Device; and

(f) set up and activated the Mobile Token and Biometric Credential Authentication Service (if applicable) according to the Bank's activation instructions using the Customer's Identity Verification Information and a one-time Password sent by the Bank to the Customer.

8. To facilitate the provision of the Mobile Token and Biometric Credential Authentication Service, the Customer agrees that the Bank may require the Customer to execute such forms and/or documents, provide such information and perform such acts as the Bank may consider reasonably necessary.

9. The Customer acknowledges that the Bank may, at its discretion, from time to time prescribe updates to the Mobile Banking App or the Website and their in-built features which must be installed in order to enable the proper functioning of the Mobile Banking App, the Mobile Token and the Biometric Credential Authentication Service. The Customer acknowledges that it is the Customer's sole responsibility to update the Mobile Banking App and/or access the latest updated version of the Website to access the Online Enterprise Banking Services using the Mobile Token and/or the Biometric Credential Authentication Service and the Bank shall not be liable to the Customer for any loss or damage caused to the Customer due to its inability to access any Online Enterprise Banking Services if the Customer fails to (A) install any required updates to the Mobile Banking App or (B) access the latest version of the Website. Notwithstanding the foregoing, the Bank does not represent or warrant that the Mobile Token and/or the Biometric Credential Authentication Service will be available at all times, be compatible with any particular device or model, software or other online banking services that the Bank may offer from time to time. The Customer shall be responsible for ensuring that the Customer's Mobile Device is a Permitted Mobile Device which meets any compatibility requirements. Failure to do so may result in malfunctioning of the Mobile Token or the Biometric Credential Authentication Service.

Provision of the Mobile Token

10. The Mobile Token is a digital security token which is offered by the Bank to Customers for the Customer as one of the means to authenticate his or her identity for accessing and/or using the Online Enterprise Banking Services on the Mobile Banking App. Customer may set up its Mobile Token on any Permitted Mobile Device by:

(a) logging on to the Mobile Banking App and accepting all applicable terms and conditions for the set-up and use of the Mobile Token;

(b) entering a Security Code which will be sent to the Customer at his or her designated mobile number registered with the Bank;

(c) designating a Mobile Token Password,

(d) (only applicable to Biometric Credential Authentication Service) applying the Customer's Biometric Credentials for authentication purposes; and

(e) (only applicable to Biometric Credential Authentication Service) where the Customer's Mobile Device carries a biometric authentication function and if the Customer has agreed to the terms and conditions under this Annex 1, enabling access to and use of the Mobile Token via the Biometric Credential Authentication Service,

or otherwise in accordance with any other steps or instructions as may be prescribed by the Bank from time to time.

11. Set up and activation of the Mobile Token involves the creation and storing of a digital security token in the Permitted Mobile Device. The Customer acknowledges that each Mobile Token may only be bound to and activated by only one Mobile Device at a time. Once a Mobile Token is bound, the Permitted Mobile Device will be recognized by the Bank for the purposes of authenticating such Customer's identity on a continuous basis in relation to the access and use of any Online Enterprise Banking Services by such Customer. The Bank shall have no obligation or duty to enquire or verify the identity or authority of any person accessing the Online Enterprise Banking Services via the use of the Mobile Token. Should the Customer wish to terminate its use of the Mobile Token or otherwise to unbind a Permitted Mobile Device, the Customer may only do so by deregistering the Mobile Token from the applicable Permitted Mobile Device under the Online Enterprise Banking Services or otherwise contacting the Bank by calling the Bank's customer hotline posted by the Bank from time to time in the Website or Mobile Banking App for assistance.

12. The Customer acknowledges that once a Mobile Token is set up and activated, the Security Device of the Customer (unless otherwise requested by the Customer) will be automatically disabled and may no longer be used to access or use any Online Enterprise Banking Services.

Provision of Biometric Credential Authentication Service (if applicable)

13. The Customer acknowledges and agrees as follows, along with the Mobile Token:

    (a) once the Biometric Credential Authentication Service (if applicable) is activated, any Biometric Credentials stored on the Customer's Permitted Mobile Device can be used to access the Online Enterprise Banking Services and use of any Mobile Token which the Customer has activated and bound to the Permitted Mobile Device. The Customer further acknowledges and accepts that any person who gains access to the biometric credentials or the biometric authentication controls of the Customer's Permitted Mobile Device will be able to access the Online Enterprise Banking Services, authenticate their use of the Mobile Token (if any) and give Instructions to the Bank in respect of the Customer's accounts, including, without limitation, withdrawing or otherwise dealing with the Customer's funds;

    (b) for the purpose of providing the Biometric Credential Authentication Service, the Mobile Banking App and its in-built features (such as any Mobile Token activated by the Customer) will interface with the biometric authentication function and data on the Customer's Permitted Mobile Device. The Customer consents to the Bank's access and use of such function and data in the Customer's Permitted Mobile Device for the provision of the Biometric Credential Authentication Service; and

    (c) the Customer will register at least one of the Customer's Biometric Credentials to control access to the Permitted Mobile Device via the Biometric Credential Authentication Service.

Security

14. The Customer acknowledges that information in relation to the Customer's accounts and/or transaction records may be stored on the Customer's Permitted Mobile Device and the Bank shall have no liability if the stored data is exposed when the Customer's Permitted Mobile Device is used by another person (whether with or without the Customer's authorisation). To protect the Customer's privacy and assets, the Customer agrees to take steps to keep confidential and secure the Customer's Permitted Mobile Device, Mobile Token Password, Passwords, and bank or account related information and to prevent unauthorised use of the Customer's Permitted Mobile Device, which include, without limitation:

    (a) ensuring that (in case of the Biometric Credential Authentication Service) only the Customer's Biometric Credentials are stored on the Customer's Permitted Mobile Device, the Customer's Permitted Mobile Device is securely and safely kept and any Password, Mobile Token Password or Security Code allowing access to altering or adding biometric credentials on the Customer's

Permitted Mobile Device is protected. The Bank will not be responsible for any losses arising out of any unauthorised transactions due to the Customer's failure to secure access to the Customer's Permitted Mobile Device;

(b) being vigilant of false matches under the facial mapping function. As an alternative, the Customer may choose to use its Identity Verification Information to access the Online Enterprise Banking Services via the Mobile Banking App, or authenticate the Customer's identity for use of the Mobile Token using the Customer's Mobile Token Password;

(c) disabling any function provided by, and refraining to consent to any settings of, the Customer's Permitted Mobile Device that would otherwise compromise the security of the use of the biometric authentication (e.g. disabling "attention-aware" feature for facial recognition);

(d) ensuring that the Customer's Permitted Mobile Device is locked immediately after use and when it is not in the Customer's possession;

(e) refraining from disclosing or sharing the Customer's Permitted Mobile Device Passwords, Mobile Token Passwords or Security Codes with any other person or allow any other person's access to the Customer's Mobile Token and/or Biometric Credentials and/or biometric authentication function on the Customer's Permitted Mobile Device;

(f) avoiding using easily accessible personal information such as date of birth, telephone number or any recognisable part of the Customer's name in setting any Password or any Mobile Token Password or use the same Password or the same Mobile Token Password to access any other services (for example, to connect to the internet or to access to the Mobile Banking App);

(g) avoiding putting down or recording any device Passwords (e.g. the Password of the Mobile Token) or Security Codes without proper safeguard;

(h) being vigilant of the Customer's surroundings before entering any Passwords, Mobile Token Password or Security Codes on the Customer's Permitted Mobile Device to ensure their secrecy;

(i) regularly changing the Passwords and Mobile Token Password of accessing the Permitted Mobile Device, the Mobile Token and Biometric Credential Authentication Service (if applicable);

(j) changing the Customer's Passwords or Mobile Token Password immediately if the Customer suspects that the Customer has been deceived by a fraudulent website, Mobile Banking App, email, or SMS/WAP push message (for example, where the Customer fails to logon to the Mobile Banking App with the use of the correct biometric credentials and/or Mobile Token Password);

(k) notifying the Bank as soon as reasonably practicable if it suspects that any of the Customer's Identity Verification Information, any other security codes (including, without limitation, the Password of the Mobile Token) and/or the Permitted Mobile Device have been compromised, lost, stolen, or accessed or used without the Customer's authorisation;

(l) strictly adhering to all security advice, measure, guidelines and instructions from time to time provided to the Customer by the Bank and/or the manufacturer of the Customer's Permitted Mobile Device applicable to the Customer's use of its Permitted Mobile Device;

(m) notifying the Bank without delay if the Customer changes the Customer's mobile phone number;

(n) upon termination of the use of the Mobile Banking App and/or the Mobile Token for any reason, removing the Mobile Banking App and/or the Mobile Token from the Customer's Permitted Mobile Device;

(o) removing the Mobile Banking App from the Customer's Permitted Mobile Device if the Customer changes or disposes of its Permitted Mobile Device;

(p) ensuring that the Mobile Token Password are kept secure and under the personal control of the Customer and will not permit any person other than the Customer to use the Mobile Token. The Mobile Token shall at all times remains the property of the Bank and issued at the Bank's discretion and the Customer shall immediately unregister or otherwise disable immediately upon the Bank's request; and

(q) notifying the Bank in the event of loss or theft of the Permitted Mobile Device to which a Mobile Token is bound as soon as reasonably practicable by telephone at such telephone number as the Bank may from time to time prescribe and confirm the same in writing if requested by the Bank. If the Customer fails to report such incidents as soon as reasonably practicable to the Bank or has otherwise acted fraudulently or with gross negligence, the Customer may be responsible for all direct losses as a result of all unauthorised transactions involving the use of, as the case may be, the lost of the Permitted Mobile Device to which a Mobile Token is bound by any person.

15. Upon the Customer notifying the Bank that the security of the Customer's Biometric Credentials, Mobile Token or other security code was suspected to be compromised, the Bank is entitled (but not obliged) to require the Customer to change the Identity Verification Information, re-set the Mobile Token, re-register the Customer's Biometric Credentials or suspend or cease the use of the Mobile Token and Biometric Credential Authentication Service.

16. The Customer shall be solely responsible for using, and shall be liable for any loss that results from any unauthorised use of the Mobile Banking App, the Biometric Credential Authentication Service and/or the Mobile Token due to the Customer's failure to adopt and maintain appropriate safeguards (including, without limitation, to the measures in Clause 14 above).

Disclaimer and limitation of liability

17. The Customer acknowledges that the biometric authentication function of the Customer's Permitted Mobile Device is not provided by the Bank, and the Bank makes no representation or warranty as to the continued accessibility, security, accuracy, functionality or performance of the biometric authentication function on the Customer's Permitted Mobile Device.

18. The Customer acknowledges that the Mobile Token and the Biometric Credential Authentication Service is for the purpose of the Customer's personal convenience. The Customer's use of the Mobile Token and/or the Biometric Credential Authentication Service is wholly at the Customer's own risk. The Mobile Token and/or the Biometric Credential Authentication Service is provided on an "as is" basis. To the maximum extent permitted by the Regulatory Requirements, the Bank disclaims all conditions, warranties (including, without limitation, any warranties of merchantability, fitness for a particular purposes, accuracy and non-infringement of third party rights), representations or other terms which may apply to the Mobile Token and the Biometric Credential Authentication Service, whether express or implied.

19. To the fullest extent permitted by the Regulatory Requirements, the Bank will not be responsible for any loss the Customer may suffer in connection with the Customer's use of the Mobile Token and/or the Biometric Credential Authentication Service, the Customer's Instructions to the Bank or any unauthorised transactions made through or in connection with the Mobile Token and/or the Biometric Credential Authentication Service.

20. To the fullest extent permitted by the Regulatory Requirements, the Bank will not be liable for any act, omission, negligence, default, damages, losses (including, without limitation, loss or leakage of data), causes of action, whether in contract, tort (including, without limitation, negligence), or otherwise arising in connection with the use of the Mobile Token and/or the Biometric Credential Authentication Service. The

Bank shall not be liable for any error, interception, corruption, deletion or inaccuracy in the Mobile Token and/or the Biometric Credential Authentication Service, any person's use of, or reliance on or inability to use the Mobile Token and/or the Biometric Credential Authentication Service, any interruption or hindrance of or delay in the operation of the Mobile Token and/or the Biometric Credential Authentication Service, any incomplete transmission, any circuit or system failure or any computer virus. The Bank shall not be responsible for any loss of profit, sales, business, revenue, business opportunity, goodwill or reputation, or any special, consequential or indirect loss or damage arising out of such act, omission, negligence or default with respect to the Mobile Token and/or the Biometric Credential Authentication Service.

21. The Customer shall hold harmless and indemnify the Bank, its officers, employees, agents and any other persons appointed by the Bank against any claims, suits, actions, proceedings, losses, damages, obligations and/or liabilities which any of them may incur or suffer, and all costs and/or expenses of reasonable amount and reasonably incurred by any of them as a result of or in connection with:

    (a) the Customer's failure to comply with the provisions of this Annex 1; or

    (b) the Customer's fraud, wilful misconduct or gross negligence in the Customer's use of the Biometric Credential Authentication Service, the Mobile Token and/or the Mobile Banking App.

Privacy

22. The Bank recognises the importance of respecting the Customer's privacy. The Customer's Biometric Credentials will not be stored or recorded by the Bank. The Bank's Privacy Policy and PDPO Notice provide information on how the Bank may collect, use, share, and protect the Customer's personal data provided to the Bank, as well as the choices, access and correction rights the Customer has in relation to its personal data.

Service availability and termination

23. The Mobile Token and/or the Biometric Credential Authentication Service may be suspended, terminated, withdrawn or amended by the Bank at any time without prior notice or providing any reason. The Bank is under no obligation to continually provide the Mobile Token and/or the Biometric Credential Authentication Service. The Bank may in its absolute discretion decide whether the Customer are eligible to use the Mobile Token and/or the Biometric Credential Authentication Service and as the Bank considers appropriate, the Bank is entitled to suspend the Customer's use of the Mobile Token and/or the Biometric Credential Authentication Service or any part of it, or suspend the Customer's access to the Mobile Token and/or the Biometric Credential Authentication Service without prior notice. The Bank's decision in this regard is final and binding on the Customer. The Bank will not be responsible for any loss or damage suffered by the Customer arising from such decisions.

Others

24. This Annex 1 may be amended at any time and from time to time. The amended terms and conditions will become effective upon the Bank giving reasonable notice to the Customer, including posting the amended terms and conditions on the Mobile Banking App, on the Website or displaying the amended terms and conditions in the Bank's branches (where appropriate). By continuing to use the Mobile Token and/or the Biometric Credential Authentication Service, subject to Regulatory Requirements, the Customer is deemed to have agreed to the amended terms and conditions.

25. This Annex 1 is governed by the laws of the Hong Kong Special Administrative Region. The Customer agrees to submit to the non-exclusive jurisdiction of the Hong Kong courts in relation to any dispute in respect of or arising from this Annex 1, but these terms and conditions may be enforced in the courts of any competent jurisdiction.

26. No person other than the Bank and the Customer will have any right under the Contracts (Rights of Third Parties) Ordinance to enforce or enjoy the benefit of any of the provisions in this Annex 1. Notwithstanding any provision contained herein, the consent of any person who is not a party to this Annex 1 is not required

to rescind or vary the terms.

27. In the event of any inconsistency between the English version and the Chinese version of these terms and conditions in this Annex 1, the English version will prevail.