

TERMS AND CONDITIONS FOR SG CYBERBANKING SERVICE (PERSONAL BANKING)

This document sets out the terms and conditions (as amended, modified and/or supplemented from time to time) (the “**Terms**”) that apply to the use of the Cyberbanking Service provided by The Bank of East Asia, Limited, Singapore Branch (the “**Bank**”).

To the extent not inconsistent with the Terms, the Bank’s Accounts and Services Terms and Conditions (the “**General Terms**”) shall be incorporated into the Terms. If there is any conflict or inconsistency between the Terms and the General Terms, the Terms shall prevail. Capitalised terms used but not defined in the Terms shall have the meaning given to them (if any) in the General Terms.

1 Definitions and Interpretation

In these Terms, the following terms, shall, except where the context requires otherwise, have the following meanings:

- 1.1 “**Account**”, in relation to a Customer, means any account held by the Customer with the Bank that is accessible via the Cyberbanking Service;
- 1.2 “**Banking Act**” means the Banking Act 1970 of the laws of Singapore;
- 1.3 “**BEA App**” means the software made available by the Bank and designated to run on smartphones and other mobile devices to provide the services as specified by the Bank from time to time;
- 1.4 “**BEA Mobile Banking**” means the banking services offered by the Bank in accordance with the Terms through electronic delivery channels including but not limited to smartphones and any other mobile devices as BEA may designate from time to time;
- 1.5 “**Biometric Authentication**” means the identity authentication function in BEA App through which biometric credentials, including but not limited to fingerprint, facial map and/or any other biometric credentials, can be accessed and used to confirm transactions in Cyberbanking, BEA App or other electronic delivery channels as designated by the Bank from time to time;
- 1.6 “**Business Day**” means a day (other than a Saturday, Sunday or a public holiday in Singapore) on which the Bank is open for business;
- 1.7 “**Contact Information**” means the personal contact information of the Customer, including without limitation the Customer’s Singapore mobile phone number, email address and/or mailing address.
- 1.8 “**Customer**” means any customer of the Bank which is a natural person who has entered into an arrangement with the Bank to use the Cyberbanking Service in their personal capacity;

- 1.9 "**Cut-Off Time**", in relation to any Business Day, means the time on that Business Day prescribed by the Bank (which the Bank may vary from time to time), by which the Bank must receive Instructions if they are to be processed by the Bank within that same Business Day;
- 1.10 "**Cyberbanking Number**" means the unique identifier number that pertains to the Customer, which when used with the PIN and OTP, will enable the Customer to access and use the Cyberbanking Service;
- 1.11 "**Cyberbanking Service**" means such services offered by the Bank over different electronic delivery channels including the BEA App, BEA Mobile Banking as prescribed by the Bank from time to time, including but not limited to the internet, mobile devices, and telephone networks;
- 1.12 "**Equipment**" means any electronic, wireless, communication, transmission or telecommunications equipment, device or medium including any computer, mobile equipment, terminal, machine, system, hardware, software (including any plug-ins and any software for Biometric Authentication), and the internet, network connection or infrastructure, which may be required to use the Cyberbanking Service and/or the Services;
- 1.13 "**High-risk Activities**" includes but is not limited to the following activities on the Customer's Account:
- a. adding of payees to the Customer's payment profile;
 - b. increasing the Transaction Limits for outgoing payment Transactions from the Account;
 - c. disabling transaction notifications that the Bank will send upon completion of a payment Transaction; and
 - d. change in the Customer's Contact Information.
- 1.14 "**Inbox Message**" means a message from the Bank that is sent to the Customer's designated mobile device or such other form(s) of electronic notification as prescribed by the Bank from time to time;
- 1.15 "**Instruction**", in relation to a Customer, means, any instructions from the Customer to the Bank given via the Cyberbanking Service, and includes requests or instructions to the Bank for making deposits, withdrawals, transfers, or payments or for information with respect to the Customer's Account(s);
- 1.16 "**i-Token**" means a device binding unique identifier which could be downloaded to BEA App of the Customer and stored in the keychain (or other security area described by the Bank from time to time) of the designated mobile device after successful registration of i-Token Service with the Bank;
- 1.17 "**i-Token PIN**" means the personal identification number designated and used by the Customer to authenticate the access to BEA Mobile Banking, Cyberbanking and other delivery channels as announced by the Bank from time to time, and to confirm transactions performed via the individual electronic delivery channels.
- 1.18 "**i-Token Service**" means the service provided by the Bank to the Customer from time to time in relation to i-Token as two-factor authentication method, to enable the Customer to use i-Token PIN/Biometric Authentication to login and/or confirm transactions in Cyberbanking and/or BEA App via the designated mobile device(s);
- 1.19 "**Limit**", in relation to an Account of a Customer, means any transactional or other limit on the amount that may be paid, transferred or withdrawn by the Customer in a single transaction or a series of transactions using the Cyberbanking Service;

- 1.20 **“Malware”** means computer viruses, bugs or other malicious, destructive or corrupting software, code, agent, program or macros, and/or phishing or social engineering schemes which utilise computer software or telecommunications to obtain Customer’s personal data or log-in credentials such as the PIN number or any other information related to the Customer for malicious or fraudulent purposes, including, without limitation, through Structured Query Language injections, cross site scripting, worms, Trojan horses, adware or spyware;
- 1.21 **“One Time Password” or “OTP”** means the code generated by the Bank and sent to a mobile device designated by the Customer and accepted by the Bank by short message service (**“SMS”**), for the purpose of authenticating the identity of the Customer and enabling the Customer using the Cyberbanking Number and the PIN, to access and use the Cyberbanking Service, or for the purpose of authorizing Transactions within the Cyberbanking Service;
- 1.22 **“Personal Identification Number” or “PIN”** means the code chosen by the Customer or set by the Bank that when used in conjunction with the Cyberbanking Number and the OTP, will enable the Customer to access and use the Cyberbanking Service;
- 1.23 **“Push Notification”** means a message, including any content or data, which is transmitted as part of the BEA App and delivered to the Customer’s Equipment;
- 1.24 **“Security Code”** means a one-time numerical code generated through i-Token Service to login and/or confirm transactions via electronic delivery channels;
- 1.25 **“Security Details”**, in relation to a Customer, means the Customer’s Cyberbanking Number, the Customer’s PIN, i-Token PIN, Security Code and/or any OTP issued by the Bank;
- 1.26 **“Seemingly Authorised Transaction”** means a Transaction which fulfils the following:
- a. The Transaction is perpetrated through the impersonation of a legitimate business or government entity (**“Impersonated Entity”**);
 - b. the scammer, pretending to be the Impersonated Entity, uses a digital messaging platform to obtain the Customer’s Security Details and/or Account details;
 - c. the Customer enters his Security Details and/or Account details on a fabricated digital platform; and
 - d. the Customer’s Security Details and/or Account details are used to perform Transactions that the Customer did not intend to be performed.
- 1.27 **“Services”** means any of the functions or services provided by the Bank to the Customer as part of the Cyberbanking Services, including without limitation, any credit or other banking facilities that may be applied for through the Cyberbanking Services and provided by the Bank to the Customer on such terms as may be determined by the Bank;
- 1.28 **“Transaction”** means a transaction effected by the Customer pursuant to or as a result of an Instruction;
- 1.29 **“Website”** means the website through which the Customer can access the Cyberbanking Service at <http://www.hkbea.com.sg>;

2 Use of the Cyberbanking Service

- 2.1 The Customer acknowledges that the Customer's access and/or use of the Cyberbanking Service shall be subject to and governed by these Terms, which the Customer is required to agree to when applying for the Cyberbanking Service or first accessing the Cyberbanking Service. Without prejudice to the foregoing, by accessing and/or using the Cyberbanking Service, the Customer is deemed to have read, understood and agreed to be bound by these Terms.
- 2.2 The Customer shall only be permitted to use the Cyberbanking Service in accordance with the Terms.
- 2.3 Upon the Customer being approved by the Bank to use the Cyberbanking Service, the Bank will assign to the Customer a Cyberbanking Number, together with such other account identification(s) in any format as may be prescribed by the Bank from time to time. The Bank shall further assign to the Customer an initial PIN, which the Customer is required to change as soon as possible after receipt. The Customer authorises the Bank to issue the initial PIN by post, physical collection at a Bank branch, or such other means as the Bank may consider appropriate.
- 2.4 The Bank may at its sole discretion introduce and provide new Services through the Cyberbanking Service from time to time. The Customer can subscribe for the new Services in such manner the Bank may prescribe from time to time by accepting all the terms and conditions of such Services, and providing such other information or documents as may be prescribed by the Bank.
- 2.5 In the event of any misuse of the PIN(s) or any purported or fraudulent use of the Cyberbanking Service by the Customer, including instances whereby online fraud is perpetrated by way of any Malware to subvert any authentication process put in place by the Bank, the Customer shall not hold the Bank liable for any loss suffered by the Customer except in the case of the Bank's:
 - a. gross negligence, fraud or wilful default;
 - b. non-compliance with any requirement imposed by MAS on the Bank in respect of its provision of any financial service; or
 - c. breach these Terms.
- 2.6 The Customer may request, in writing or through the Cyberbanking Service, for a change in the PIN from time to time. For the avoidance of doubt, the issuance of a new PIN by the Bank, the selection of a new PIN by the Customer, or the usage of such new PIN shall not be construed as creating or establishing a new Account or contract between the Customer and the Bank.
- 2.7 The Customer understands and acknowledges that the Cyberbanking Service is provided by the Bank as an additional means through which the Customer may effect banking transactions with the Bank and shall not be considered a substitute for other method(s) of effecting banking transactions. In the event that the Cyberbanking Service is not available for any reason whatsoever (whether or not such unavailability is or is not within the control of the Bank), the Customer shall have no claim whatsoever against the Bank but shall use other available means to effect banking transactions with the Bank.
- 2.8 The Bank shall use all reasonable endeavours to ensure that information made available by the Cyberbanking Service is correct and updated at regular intervals. All information with respect to the Customer's Transactions and the Accounts that are provided via the Cyberbanking Service are provided on with an understanding of the inherent risks of the internet medium. The Customer accepts and agrees that, in the event of errors or

inaccuracies, information reflected within the Bank's own internal records shall, in the absence of manifest error, prevail over any information provided via the Cyberbanking Service.

- 2.9 The Customer shall provide to the Bank all Contact Information as may be reasonably required by the Bank to provide the Services to Customer.
- 2.10 The Customer represents, warrants and undertakes that all information (including Contact Information) provided by the Customer to the Bank in relation to the Cyberbanking Services shall be and remain at all times true, complete and up-to-date. The Customer must notify the Bank of any change in their information as soon as reasonably practicable. The Bank shall bear no liability or responsibility for any claims to the extent that there has been a breach of this clause by the Customer.
- 2.11 The Bank may send notices, information, documents, communications and risk warning messages ("**Notifications**") to Customer at any time. Such Notifications may relate to payment Transactions (outgoing) on Customer's Account, the activation of Customer's i-Token, any High-risk Activities on the Customer's Account, sending any Security Details to the Customer, or such other activities as may be relevant or necessary to be notified to Customer from time to time. Any Notifications will be sent to the Customer via one or more of the following methods:
 - a. Push Notifications;
 - b. SMS; or
 - c. Email.
- 2.12 The Bank will provide the Customer with Notifications in respect of all payment Transactions(outgoing), regardless of the amount.
- 2.13 The Customer shall take all steps necessary to (i) allow the Cyberbanking Service to send Notifications and (ii) monitor the Notifications sent to the Customer's Equipment, including enabling Push Notifications and providing the Bank with Customer's Contact Information in accordance with clauses 2.9 and 2.10 above. The Customer undertakes to read all Notifications before completing any outgoing payment Transactions or High-risk Activities.
- 2.14 The Customer is responsible for ensuring that it fully understands the risk and implications of performing outgoing payment Transactions or High-risk Activities, as will be disclosed by the Bank to the Customer in the relevant Notification at the point before the Customer performs such outgoing payment Transactions or High-risk Activities. When in doubt, the Customer should contact the Bank and/or refer to the Bank's Website for more information. The Customer is deemed to have understood the risks and implications of such transactions as presented by the Bank in the relevant Notification.
- 2.15 In the event that an i-Token is activated on a device, the Bank will impose a cooling off period of twelve (12) hours, during which High-risk Activities cannot be performed.

3 i-Token Service

- 3.1 i-Token provides an alternative means of verifying the Customer's identity for accessing the Cyberbanking Service and other delivery channels as announced by the Bank from time to time. The Customer may register for i-Token Service on such mobile devices as may be specified by the Bank from time to time by completing the steps specified by the Bank. Once successfully registered, the Customer may use the i-Token to confirm their identity for

accessing the Cyberbanking Service, to the extent such i-Token access is made available by the Bank.

- 3.2 If there is any change to the Customer's designated mobile device for the i-Token Service, the Customer should follow the procedures for installing and activating the i-Token on the Customer's new mobile device, as prescribed by the Bank from time to time.
- 3.3 Updates to the i-Token may be required periodically. The Customer may not be able to use the i-Token Service if the latest version of BEA App has not been downloaded to the Customer's designated mobile device(s) for i-Token Service.
- 3.4 The Customer agrees and understands that the Bank will send an Inbox Message to the BEA App for redirecting to login to different electronic delivery channels or to confirm transactions using i-Token PIN or Biometric Authentication. The Bank shall only notify the Customer in respect of any transactions pending for confirmation via Inbox Message. The Customer shall check for Inbox Messages on the BEA App regularly from time to time and contact the Bank if any expected notifications are not received.
- 3.5 Inbox Messages shall be deemed to be received by the Customer immediately after transmission.
- 3.6 Any instructions or transactions confirmed or executed by the Customer via the Customer's registered credentials on the i-Token Service may not be rescinded or withdrawn. All such instructions or transactions, when confirmed and acknowledged by the Bank, shall be irrevocable and binding on the Customer regardless of whether or not such instructions or transactions are confirmed or executed by the Customer or by any other person purporting to be the Customer. The Bank shall be under no duty to verify the identity or authority of the person giving any such instructions or signing such transactions or the authenticity of such instructions or transactions which shall be conclusive and binding on the Customer in any event.
- 3.7 The Bank may at all times and from time to time in its sole discretion without having to state the grounds for such refusal and without any liability whatsoever, refuse to act upon any instructions or transactions confirmed or executed by the Customer via i-Token as the Bank thinks appropriate.
- 3.8 Upon receiving any Inbox Message or Push Notification from the Bank through BEA App, the Customer shall examine the Inbox Message or Push Notification on a timely basis and take follow-up action accordingly. Any Instruction or transaction may be considered in the Bank's discretion to be incomplete or invalid if the relevant Instruction or transaction is not confirmed by the Customer via i-Token by the stipulated time.
- 3.9 The i-Token Service is provided by the Bank subject to such restrictions as may be notified by the Bank from time to time. In particular, not all types of accounts are eligible to use the i-Token Service.
- 3.10 If the Customer believes that the security of their i-Token has been compromised, the Customer must cease the use of the Cyberbanking Service, change the relevant passwords, activate the "Suspend Account" feature to disable and block access to the Customer's Cyberbanking Account(s), i-Token and Biometric Authentication and notify the Bank immediately. The Bank may require the Customer to change the relevant passwords and/or the i-Token registered in their mobile device, to cease and/or re-enable the use of the Cyberbanking Service and/or i-Token Service.

4 Biometric Authentication

- 4.1 Biometric Authentication provides an alternative means of verifying the Customer's identity for accessing BEA Mobile Banking or other applicable elements of the Cyberbanking Service. The Customer may register their mobile device (with biometric sensor supported) that meets the technical for Biometric Authentication by completing the registration steps specified by the Bank.
- 4.2 By registering to use Biometric Authentication or using Biometric Authentication, the Customer accepts and agrees that the Biometric Authentication Service will access the biometric credentials (including but not limited to fingerprint, facial map and/or any other biometric credentials as prescribed by the Bank from time to time) recorded and stored in the Customer's mobile device which has been successfully registered for Biometric Authentication, and the Customer hereby consents to the Bank accessing and using such information for the purposes of Biometric Authentication, including to authenticate the identity of the Customer.
- 4.3 Once the Customer has successfully enabled and registered for Biometric Authentication in their mobile device, the Customer may use their biometric credentials registered with Biometric Authentication to confirm their identity for accessing Cyberbanking Service, to the extent such Biometric Authentication access is made available by the Bank.
- 4.4 The Customer must not use facial recognition for Biometric Authentication if the Customer (i) has identical siblings, or (ii) is an adolescent where their facial features may be developing rapidly. The Customer must not compromise or disable the security settings of their biometric credentials registered in the Customer's mobile device, including but not limited to disabling passcode to access the biometric credentials, and/or disabling "attention aware" features for facial recognition. Biometric Authentication is provided for the Customer's personal use only.
- 4.5 To use Biometric Authentication, the Customer shall ensure that the BEA App has been installed on their mobile device and be a valid user of BEA Mobile Banking. The Customer acknowledges that the availability of Biometric Authentication is subject to the compatibility and technical specifications of their mobile device.
- 4.6 Any instructions or transactions confirmed or executed by the Customer via Biometric Authentication may not be rescinded or withdrawn. All such instructions or transactions, when confirmed and acknowledged by the Bank, shall be irrevocable and binding on the Customer regardless of whether or not such instructions or transactions are confirmed or executed by the Customer or by any other person purporting to be the Customer. The Bank shall be under no duty to verify the identity or authority of the person giving any such instructions or signing such transactions or the authenticity of such instructions or transactions which shall be conclusive and binding on the Customer in any event.
- 4.7 If the Customer believes that the security of their biometric credential(s) has been compromised, the Customer must cease the use of the Cyberbanking Service, change the relevant passwords, activate the "Suspend Account" feature to disable and block access to the Customer's Cyberbanking Account(s), i-Token and Biometric Authentication and notify the Bank immediately. The Bank may require the Customer to change the relevant passwords and/or biometric credential(s) registered in their mobile device, to cease and/or re-enable the use of Cyberbanking Service and/or Biometric Authentication.

5 Security

- 5.1 Each time the Customer accesses the Cyberbanking Service, the Customer will be required to provide its Cyberbanking Number and PIN. After the PIN is entered, the Bank will, as an

additional login authentication measure, generate the OTP and send the same by SMS to a mobile device the number of which is registered by the Customer with the Bank. After the Customer has logged in to the Cyberbanking Service, in case of certain transactions (as may be decided by the Bank), further verification via, i-Token, Biometric Authentication, or an OTP generated by the Bank may be required. The Customer agrees that it shall not be entitled to access the Cyberbanking Service and/or effect any Transaction until it has completed such further verification as may be required by the Bank.

- 5.2 The Customer agrees that it shall keep all Security Details confidential and take all reasonable precautions to prevent unauthorised or fraudulent use of the Cyberbanking Service.
- 5.3 The Customer shall not use public access computer terminals, such as those available in internet cafes, or any other shared or unsecured computer or mobile devices to access the Cyberbanking Service unless he is satisfied that there are sufficient internet security arrangements in place. In the event that the Customer chooses to access the Cyberbanking Services through any such unsecured Equipment, the Customer shall be fully responsible for all loss or damage which it may suffer as a result, and shall further indemnify the Bank against all loss or damage which the Bank may suffer as a result.
- 5.4 The Customer shall close all other browser windows before logging into the Cyberbanking Service to reduce the risk of unauthorised access from other websites.
- 5.5 For the Customer's own protection, the Customer agrees that it shall not disclose any of its Security Details to anyone (including the Bank's employees) or to any unknown or suspicious websites, and shall not keep any record (physical or electronic) of any Security Details in a manner that allows any third party to easily misuse the Security Details. The Customer acknowledges that the Bank and/or its employees will never ask the Customer to disclose any of their Security Details in any form or manner, either by email, telephone or in writing. The Customer acknowledges that fraudsters may use various means (including malicious software) to elicit such information and undertakes that if the Customer has reasons to believe that any of its Security Details have been compromised, the Customer shall notify the Bank immediately without any delay.
- 5.6 The Customer undertakes to change the initial PIN as soon as possible after receipt from the Bank.
- 5.7 The Customer undertakes to change their PIN immediately if they suspect that the security of their PIN has been compromised.
- 5.8 The Customer acknowledges that it is a good practice to change the PIN regularly.
- 5.9 The Customer acknowledges that it is not advisable to write down the PIN in a prominent place, disseminate the PIN by unsecure means of communications (such as emails) or to use the same PIN to access other websites, internet applications or services provided by other parties.
- 5.10 The Customer agrees to take all reasonable precautions and be alert to the surrounding environment when accessing the Cyberbanking Service to ensure that the Security Details are not inadvertently disclosed or revealed to any other person.
- 5.11 The Customer undertakes to check the bank balances of the Accounts and information concerning its Transactions for irregular or unauthorised transactions regularly. If the Customer has reason to believe that fraudulent, unauthorised or suspicious Transactions have been carried out on any Account, the Customer undertakes to notify the Bank immediately.

- 5.12 At the Customer's request, the Bank shall provide the Customer with relevant information of all unauthorised Transactions executed on the Customer's Account, including without limitation the transaction dates, transaction timestamps and parties to the transaction.
- 5.13 The Bank reserves the right to detect and block suspected fraudulent or unauthorised Transactions at any time, regardless of whether the Customer has notified the Bank of such Transactions. The Bank may, in its sole discretion, inquire into the authenticity of such Transactions before allowing them to be executed. Without limiting the generality of the foregoing, the Bank reserves the right to:
- a. block any payment Transaction that would result in an Account being rapidly drained of a material sum, and all subsequent payment Transactions to the suspected recipient until the Bank obtains further verification from the Customer; or
 - b. send a notification to the Customer and block or hold for at least 24 hours:
 - (i) the outgoing payment Transaction that would result in the Account being rapidly drained of a material sum; and
 - (ii) all subsequent outgoing payment Transactions to the suspected recipient.

For the avoidance of doubt, this excludes recurring standing instructions, recurring GIRO/eGIRO deductions, bill payments to billing organisations maintained by the Bank (save for payments of bills for credit cards issued by other financial institutions), debit card Transactions, and intrabank transfers to the Customer's other account(s) within the Bank.

- 5.14 The Bank shall review the effectiveness of its detection parameters for suspected fraudulent or unauthorised Transactions on an annual basis, or as and when material triggers arise.
- 5.15 If the Bank suspects that any fraudulent or unauthorised Transactions are being carried out on an Account, the Bank reserves the right to suspend or withdraw all or part of the Cyberbanking Service.
- 5.16 The Customer acknowledges that it is important to 'log off' from the Cyberbanking Service using the logout button and to close the browser once it has finished using the Cyberbanking Service. The Customer acknowledges that for added security, the Cyberbanking Service will 'log off' automatically if the Customer's session has been inactive for more than 5 minutes.
- 5.17 The Customer acknowledges that it will clear the browser cache each time after it accesses the Cyberbanking Service.
- 5.18 The Customer shall not leave their Equipment unattended while using the Cyberbanking Service.
- 5.19 The Customer shall access the Cyberbanking Service only via the Website or BEA App and shall avoid clicking on any hyperlink embedded in any electronic email, search engines or from any unknown source to access the Cyberbanking Service. It is possible that websites can be 'cloned' to appear like the real site. The Customer shall type the address of the Website carefully into the Customer's browser to access the Cyberbanking Service. If the website appears different in any way, the Customer shall contact the Bank to report the incident as soon as possible.
- 5.20 The Bank will not send any clickable links or Quick Response ("QR") codes to the Customer (whether via email or SMS) unless:
- (a) it is a clickable link or QR code that only contains information for the Customer and does not lead to a: (i) website where the Customer is required to provide his Security Details

- or perform any payment transaction; or (ii) platform where the Customer is able to download and install apps; and
- (b) the Customer is expecting to receive the email, SMS or Push Notification from the Bank.

As such, the Customer should not click on any links or scan any QR codes purportedly sent by the Bank unless the Customer is expecting to receive information regarding products and services via these clickable links or QR codes from the Bank. The contents of these clickable links or QR codes should not lead to the Customer providing any Security Details, performing a payment transaction, or engaging in any High-risk Activities. If the Customer receives unsolicited clickable links or QR codes, Customer should immediately verify their authenticity with the Bank before taking any action.

- 5.21 The Bank will not send any phone numbers to the Customer via SMS unless the Customer is expecting to receive such SMS from the Bank.
- 5.22 The Customer shall set a strong PIN of no less than eight (8) characters and comprising a mixture of letters and numbers. The Customer further undertakes to avoid adopting a PIN that is easy to guess, that comprises of personal information (such as NRIC number, passport number, telephone number, date of birth, driving licence number or name), or any simple sequence (such as 12345678 or ABCDEFGH) or that involves using the same alphanumeric characters multiple times (such as 11111111 or A1A1A1A1).
- 5.23 The Customer shall take reasonable endeavours to remove file and printer sharing options on the Customer's computer, especially when the Customer has internet access via cable modem, broadband connection, wireless connection, or other similar set-ups.
- 5.24 The Customer shall take precautionary measures to protect the computer which it uses to access the Cyberbanking Service from hacking and virus attacks. The Customer shall regularly update its browser and the operating system of its computer with the latest security patches. The Customer shall install proper firewalls, anti-spyware and anti-virus software on its computer and update them with security patches or newer versions on a regular basis to strengthen the security of the Customer's computer. The Customer shall not set the option on its web browser to store passwords. The Customer shall take all reasonable precautions when sending or reading emails, opening attachments, or downloading files and programs. The Customer shall not open attachments received from strangers. The Customer shall not use or install any software or run programs of unfamiliar or suspicious origins. It is recommended that the Customer shall always disconnect from the internet when the Customer is not using the computer.
- 5.25 The Customer shall take all precautionary measures to protect the mobile device he uses to receive the OTP and shall never leave it unattended or share it with third parties.
- 5.26 The Customer must not do or attempt to do any of the following: (a) decompile, reverse-engineer, translate, convert, adapt, alter, modify, enhance, add to, delete or in any way tamper with the Cyberbanking Service (or any part thereof); and (b) gain access to the Cyberbanking Service (or any part thereof) in any manner other than specified by the Bank.
- 5.27 The Bank shall not in any event be liable for any loss or damage whatsoever suffered by the Customer as a consequence of the Customer's failure to observe and comply with any of the security precautions set out in this clause 5.

6 Acting on the Customer's Instructions

- 6.1 The Customer acknowledges that all Instructions transmitted to the Bank through the Cyberbanking Service shall not be considered as having been received and executed by the Bank until the Bank has received and executed such Instructions in accordance with the Bank's usual procedures and practices.
- 6.2 The Customer authorises the Bank to accept and act on any Instructions associated with the Customer's Security Details, i-Token, or Biometric Authentication that the Bank receives through the Cyberbanking Service. The Customer agrees to be bound by all Instructions reasonably received and acted upon by the Bank in good faith. The Bank shall be under no duty to inquire into or verify the authenticity of any Instructions given through the Cyberbanking Service. Beyond the authentication measures set out in the Terms, the Bank shall also be under no duty to authenticate the identity or authority of the person(s) giving or purporting to give such Instructions through the Cyberbanking Service.
- 6.3 The Bank shall be entitled to treat in good faith all Instructions received from the Customer (or person(s) purporting to be the Customer) as fully authorised and binding on the Customer regardless of the circumstances prevailing at the time the Instructions are given or the nature or amount of the Transaction and notwithstanding any error, misunderstanding, lack of clarity, errors in transmission, fraud, forgery or lack of authority in relation to the Instructions. The Customer agrees that the Customer shall be under an express duty to the Bank to prevent any fraudulent, forged or unauthorised Instructions being given.
- 6.4 All Transactions entered into pursuant to the Instructions given to the Bank through the Cyberbanking Service shall be subject to the terms and conditions governing such Transactions as may be prescribed by the Bank from time to time.
- 6.5 The amounts that the Customer shall be permitted to transfer through the Cyberbanking Service shall be subject to various Transaction Limits including but not limited to the withdrawal Limit and signing limit expressed in SGD or its equivalent as published by the Bank from time to time. The Bank shall have the right to impose such restrictions as the Bank thinks fit for the efficient operation of the Cyberbanking Service or for any other reason.
- 6.6 Given the inherent risks of communications via the internet, the Customer agrees that the Bank may from time to time in its sole discretion and without any liability whatsoever, refuse to act upon any Instructions or such part thereof as the Bank thinks appropriate, without having to provide in detail the reasons for its refusal.
- 6.7 In the event that the Bank receives an Instruction that the Bank considers to be inconsistent with any previous Instruction which has not been executed, the Bank may, at its sole and absolute discretion, refuse to act on either of such Instructions unless and until either one of such Instructions has been revoked or withdrawn to the satisfaction of the Bank.
- 6.8 The Bank shall not be liable for any delay in carrying out the Customer's Instructions if such delay is occasioned by the conduct of checks relating to prevention of money-laundering or terrorist-financing, fraud or crime prevention or other regulatory compliance matters.
- 6.9 The Bank shall not be responsible for any loss or damage (direct or incidental, and howsoever caused) which the Customer may suffer as a result of a rejection of any Instruction given through the Cyberbanking Service, if the Bank is otherwise lawfully entitled to decline to carry out the Instructions of the Customer.
- 6.10 The Bank will only accept Instructions given through the Cyberbanking Service insofar as it is (in the Bank's opinion) practicable and reasonable to do so, having regard to its business practices and procedures. The Customer acknowledges that the Bank must comply with all

laws, rules, regulations, guidelines, requests and/or recommendations of any government or regulatory authority in Singapore or elsewhere responsible for regulating the conduct of banking business and/or the provision of financial services generally. The Customer agrees that the Bank has the right to impose conditions or vary existing conditions for the provision of the Services or for the acceptance of any Instructions.

- 6.11 The Bank shall have no responsibility or obligation for any errors or omissions arising from the failure of the Customer to provide or input sufficient or accurate data to enable any Transaction to be effected through the Cyberbanking Service.
- 6.12 The Bank shall not be obliged to accept Instructions to make payment if there are, at the time of payment, insufficient funds available in the relevant Account from which payment is to be made, nor shall the Bank be obliged to give prior notice to the Customer before refusing such Instructions.

7 Timing of Instruction

- 7.1 On any Business Day, Instructions received through the Cyberbanking Service before the Cut-Off Time on that Business Day will, in the absence of exceptional circumstances, be processed by the Bank within the same Business Day.
- 7.2 Instructions received on a Business Day after the Cut-Off Time for that Business Day, and Instructions received at any time on a non-Business Day will, in the absence of exceptional circumstances, be processed by the Bank by the next Business Day.
- 7.3 If the Bank rejects any instructions, the Customer will receive notification via the Cyberbanking Service or via other means as the Bank considers appropriate.
- 7.4 In the case of any Transaction involving a fund transfer, whether interbank or intrabank, from an Account held by the Customer to any other account (whether held by the Customer or otherwise), the Bank as the paying bank shall have no responsibility to the Customer as payer as to the time when the funds will be credited to and become available in such other account. In the case of any Transaction involving a fund transfer, whether interbank or intrabank, to an Account held by the Customer from any other account (whether held by the Customer or otherwise), the time when the funds will be credited into and become available in such Account shall be in accordance with the Bank's business practice and procedures. The Bank shall have the right at any time to reverse any credit to such Account if the paying bank fails for any reason to make payment to the Bank.
- 7.5 The Customer understands that due to the inherent risks of communications through the internet, even with security arrangements in place, the internet is not a fully secure or reliable means of communication, and that this is beyond the control of the Bank. The Customer therefore acknowledges that transmission delays or failures, incorrect or incomplete data transmissions, execution delays or failures may be experienced from time to time, and agrees that Bank will not be held responsible for any loss or damage as a result thereof.

8 Operating Joint Accounts

- 8.1 If the Account of the Customer is a joint account, the Customer acknowledges that the Cyberbanking Service does not provide for more than one individual to authorise a Transaction and that the Bank is accordingly authorised to act on the Instructions of any one of the holders of that Account, notwithstanding anything provided in the terms and conditions applicable to the joint account, either by virtue of the General Terms or otherwise.

- 8.2 Where Instructions are given through the Cyberbanking Service in respect of an Account which is a joint account, each and every one of the holders of the joint account shall be bound by these Terms and shall be jointly and severally responsible for all Transactions in the Account. Notifications provided under Clause 2.11 of these Terms shall be sent to the joint account holder who initiated the outgoing payment Transaction only. Any notice given to any one of the joint account holders shall be deemed effective notice to all of the joint account holders.
- 8.3 Notwithstanding any other provisions in the Terms, the Bank reserves the right to reject Instructions given through the Cyberbanking Service or to suspend the Cyberbanking Service for an Account that is a joint account in certain circumstances (including but not limited to the following):
- a. Where the Bank becomes aware that there is a dispute between the joint account holders;
 - b. Where the Bank has been asked or directed (through any means) not to accept Instructions from any of the joint account holders; or
 - c. Where the Bank believes, in its sole discretion that a certain Transaction requires a joint decision by all the joint account holders, and the Instructions do not represent or adequately represent the decision or intent of the joint account holders.
- 8.4 Where the Account of the Customer is a joint account, any liability for losses incurred by the Customer shall apply jointly to each joint account holder.

9 The Customer's Responsibilities and Liability

- 9.1 The Customer shall as soon as possible notify the Bank in writing of any changes of address, mobile device number used for receiving the OTP or other Contact Information, which the Bank may use for the purpose of sending confirmations and other communications. Until any such change is notified by the Customer and acknowledged by the Bank, the Bank shall be entitled to continue to act on the basis of existing Contact Information in its possession.
- 9.2 Subject to Clause 9.3 below and without prejudice to other provisions hereof, the Customer agrees to indemnify the Bank against all or any losses on a full indemnity basis which is directly or indirectly related to or in connection with the use of the Cyberbanking Service, whether such use is authorised or otherwise.
- 9.3 The Customer is not liable for:
- (a) any actual loss arising from an unauthorised Transaction if the loss was due to any action or omission by the Bank and/or its employees, such as fraud or gross negligence by the Bank or its employees, or non-compliance with any obligation under these Terms; and/or
 - (b) the first SGD1,000 of any actual loss arising from an unauthorised Transaction if the actual loss arises from any action or omission by a third party (i.e., not the Bank or the Customer),
- provided that the loss does not arise from the Customer's failure to comply with any obligation under these Terms.
- 9.4 Notwithstanding Clause 9.3 above, if the actual losses incurred by the Customer arise out of a Seemingly Authorised Transaction, the Bank, along with the Customer's telecommunications company (if applicable), will conduct an investigation to determine who will bear the loss from such Seemingly Authorised Transaction, in accordance with the Shared Responsibility Framework ("**SRF**") jointly published by the MAS and Infocomm Media Development Authority.

- 9.5 The Customer must notify the Bank as soon as possible in accordance with Clause 15.3 below if any of the Customer's Security Details have been stolen or are liable to misuse or if the Customer suspects or discovers that there has been unauthorised access to/an unauthorised Transaction (including a Seemingly Authorised Transaction) on the Customer's Account via the Cyberbanking Service. The Bank may at its discretion require the Customer to confirm in writing the notification made via telephone.
- 9.6 The Customer shall only contact the Bank through contact details obtained from official sources such as the Monetary Authority of Singapore's ("MAS") Financial Institutions Directory ("FID") and the BEA App and/or Website.
- 9.7 The Customer shall make a police report as soon as practicable if so requested by the Bank and/or if the Customer suspects that he is a victim of scam or fraud. The Customer undertakes to cooperate with the police and provide evidence as far as practicable, and furnish the police report to the Bank within three (3) days of the Bank's request to do so.
- 9.8 In the event that there is a dispute regarding a Transaction, the Customer hereby agrees that the Bank may inform the police and the Customer will be required to cooperate with the Bank and the police during any investigations. The Customer hereby agrees and authorises the Bank to provide the police and/or the Bank's insurers with any information that the Bank or the police considers relevant to the investigation.
- 9.9 The Customer shall notify the Bank immediately if he suspects or discovers any erroneous Transactions from or to his Account(s). In respect of erroneous Transactions from the Customer's Account, the Bank shall work with the recipient's financial institution and make reasonable efforts to recover the sums sent in error by the Customer. The Customer shall provide the Bank with any information as may be requested by the Bank to assist it with recovering the sums sent in error by the Customer. Notwithstanding the foregoing, the Customer agrees that he shall be liable for all erroneous Transactions and Services undertaken by the Customer under the Cyberbanking Service, and the Bank will not be liable for any error not attributable to the Bank whatsoever therein and any consequence arising therefrom.
- 9.10 The Customer shall only be able to access the Cyberbanking Service if the Equipment the Customer uses is compatible with the Bank's minimum technical specifications. For full details of these requirements, the Customer may refer to the Bank's Frequently Asked Questions (FAQ) that is posted on its Website and may also be accessed from within the Cyberbanking Service. The Bank reserves the right to change the minimum technical specifications from time to time. The Customer shall ensure that its Equipment remains in good working order and is free from viruses and other harmful software or defects.
- 9.11 All costs and expenses associated with obtaining and maintaining suitable Equipment to access the Cyberbanking Service shall be borne by the Customer solely.

10 Mobile Device(s)

- 10.1 The Customer must comply with all applicable laws and regulations governing the installation, download and/or access of i-Token Service, BEA App, BEA Mobile Banking and/or the Cyberbanking Service. The Customer shall be the sole owner of their designated mobile device(s) and must not use or allow any other person to use the i-Token, Biometric Authentication, BEA App, BEA Mobile Banking and/or the Cyberbanking Service for any unauthorised purpose. Save as expressly provided for under these Terms, the Bank shall not be liable for any losses or any other consequences suffered or incurred by the Customer

as a result or arising out of the Customer's failure to comply with the aforesaid requirement or these Terms.

- 10.2 The Customer undertakes to take all reasonable precautions to keep safe and prevent fraudulent use of their designated mobile device(s) and its security information. Non-compliance of security precautionary measures as prescribed by the Bank from time to time would render the Customer liable for all actual losses arising from any unauthorised Transactions, up to the applicable Transaction Limit that the Customer and the Bank have agreed upon. The Bank may in its sole discretion update the security precautionary measures in relation to i-Token, Biometric Authentication, BEA App, BEA Mobile Banking and/or Cyberbanking Service and the Customer shall at all times follow such security precautionary measures accordingly.
- 10.3 The Customer must not access or use i-Token Service, Biometric Authentication, BEA App or Cyberbanking Service through any device or operating system that has been modified outside the mobile device or operating system vendor supported or warranted configurations. This includes but is not limited to devices that have been "jail-broken" or "rooted". A jail broken or rooted device means one that has been freed from the limitations imposed on it by the designated mobile service provider and the phone or device manufacturer without their approval. Access or use of i-Token Service, Biometric Authentication, BEA App or Cyberbanking Service on a jail broken or rooted device may compromise security and lead to fraudulent transactions. Use of i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking and/or Cyberbanking Service in a jail broken or rooted device is entirely at the own risk of the Customer. The Bank shall not be liable for any losses or any other consequences suffered or incurred by the Customer as a result thereof.
- 10.4 The Customer shall:
- a. only download and install BEA App from official sources such as the [Apple App Store and Google Play Store]; and
 - b. not download and install any applications from third-party websites outside of official sources such as the [Apple App Store and Google Play Store] and shall not download any sideloaded apps.
- 10.5 The Customer shall acquire appropriate mobile device(s) with requisite specifications and system requirement which enables i-Token Service, Biometric Authentication, BEA Mobile Banking and/or BEA App to be installed and used therein and undertake to ensure that such mobile device(s) shall not cause any damage to i-Token Service, Biometric Authentication, BEA Mobile Banking and/or BEA App whether by virus, other contaminating or destructive properties or by any reasons whatsoever. The Customer shall also procure installation of the updates and the latest version of i-Token, Biometric Authentication and BEA App in the designated mobile device(s) from time to time.
- 10.6 The Customer agrees and acknowledges that installation and registration for i-Token Service and/or Biometric Authentication are generally free-of-charge but the Bank reserves the right to levy fees and charges against the Customer to cover the running and operating costs for i-Token Service and Biometric Authentication in the future. The Customer shall be solely responsible for any fees or charges that their telecommunication carrier may charge in connection with the transmission of data or the use of i-Token Service and Biometric Authentication.
- 10.7 The Customer acknowledges that the Bank may collect, store and use technical data and related information, including but not limited to information about the designated mobile device(s), system and application software, peripherals and other personal information that is gathered periodically to facilitate the provision of software updates, product support and

other services (if any) related to i-Token Service, Biometric Authentication, BEA Mobile Banking and/or BEA App. The Bank may use such information, as long as it is in a form that does not personally identify the Customer to improve its products or to provide services or technologies.

- 10.8 The Customer understands the need to protect their mobile device, including but not limited to set a strong passcode on their mobile device and not permit any other persons to register their biometric credentials in their mobile device and/or use i-Token Service or Biometric Authentication.
- 10.9 Each mobile device may only bind one i-Token and one set of biometric credentials for Biometric Authentication.

11 The Bank's Responsibilities and Liabilities

- 11.1 The Bank shall ensure that its Website address and contact details are listed on the MAS FID and other official sources are accurate and up to date.
- 11.2 The Bank shall use all reasonable endeavours to keep the Cyberbanking Service running smoothly and to ensure the continuous delivery of the Cyberbanking Service or reasonable alternatives where necessary. However, the Bank takes no responsibility for, and will not be liable for, the Cyberbanking Service (whether in whole or in part) being temporarily unavailable due to any causes that is beyond the Bank's control, delay or failure of any communication network or any party providing such access, or any other unavoidable events.
- 11.3 The Customer accepts that i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking and Cyberbanking Service may be subject to various information technology risks or force majeure events beyond the Bank's control, including but not limited to:
- a. inaccuracy, interruption, interception, mutilation, disruption, unavailability, delay or failure relating to data transmission, communication network or internet connection;
 - b. unauthorised access by other persons (including hackers);
 - c. damage to the designated mobile device(s) caused by virus, other contaminating or destructive properties or by any reasons whatsoever;
 - d. malfunction, breakdown or inadequacy of equipment, installation or facilities; or
 - e. failure to provide i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service by the Bank due to strikes, power failures, change in law, rules or regulations or other calamity.
- 11.4 The Bank and its subsidiaries, affiliates, agents and employees shall not be liable for the occurrence of any of the events as described in clause 11.3 above or any breach or failure to perform the Bank's obligations due to abnormal and unforeseeable circumstances, fraud or negligence by the Customer, or any other causes beyond the Bank's reasonable control or anticipation. Under no circumstances shall the Bank be liable to the Customer for any incidental, indirect or consequential or exemplary damages including, without limitation, any loss of use, revenue, profits or savings (whether foreseeable by the Bank or not) arising out of or related to the access or use of i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service. The Bank's maximum liability (if any) to the Customer for loss in relation to the provision of i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service shall be limited to the amount of the relevant Transaction Limit that the Customer and the Bank have agreed upon.
- 11.5 i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking and Cyberbanking Service are provided on an "as is" basis with no representation, guarantee or agreement of any kind as to their functionality. The Bank cannot guarantee that no viruses or other

contaminating or destructive properties will be transmitted or that no damage will occur to the designated mobile device(s). Save as expressly provided for under these Terms, the Bank shall not be responsible for any loss suffered by the Customer or any third party as a result of the access or use of i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service by the Customer.

- 11.6 The Bank expressly excludes any guarantee, representation, warranty, condition, term or undertaking of any kind, whether express or implied, statutory or otherwise, relating to or arising from the use of i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service or in relation to the processing of or any other request relating to the i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service. Without prejudice to the foregoing, the Customer understands and acknowledges the acceptance by the Bank of their submission of a request through use of the i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service does not amount to a representation or warranty by the Bank that:
- a. the i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service will meet the Customer's requirements;
 - b. the i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service will always be available, accessible, function or inter-operate with any network infrastructure, system or such other services as the Bank may offer from time to time; or
 - c. the use of the i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service or the Bank's processing of any request will be uninterrupted timely, secure or free of any virus or error.
- 11.7 The Bank shall not assume any responsibility or obligation for any transaction or error due to the failure of the Customer to provide or input sufficient or accurate data which result in the relevant transaction failing to be materialised or effected through i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service.
- 11.8 The Bank shall be entitled to exercise any of its rights and remedies under these Terms (including the right to withdraw, restrict, suspend, vary or modify i-Token Service, Biometric Authentication, Cyberbanking, BEA Mobile Banking, BEA App and/or other software (whether in whole or in part)).
- 11.9 The Bank may make available on its Website or on the BEA App hyperlinks to other websites which are not under the Bank's control. The Bank does not investigate, verify, monitor or endorse the content, accuracy, or any opinions expressed within these third party websites, and such hyperlinks are provided solely for the Customer's convenience.
- 11.10 The Bank may, from time to time, temporarily suspend the Cyberbanking Service in order to carry out maintenance work or to implement updates and upgrades. The Bank shall ensure that any maintenance work, updates and/or upgrades on the Cyberbanking Service are not performed during periods when a high volume of Transactions is expected. The Bank shall use its best effort to let the Customer know in advance the specific times when the Cyberbanking Service would not be available. During such time where the Cyberbanking Service is temporarily suspended, the Bank shall ensure that the following services will continue to be provided to the Customer:
- a. The Customer's access to these Terms;
 - b. The provision of Notifications to the Customer in accordance with Clause 2.12 above;
 - c. A twelve (12) hour cooling off period after an i-Token is activated on a device, in accordance with Clause 2.15 above;
 - d. A reporting channel for the Customer to report any loss, misuse of Biometric Authentication, theft or unauthorised use of the designated mobile device(s) or

unauthorised use of the Customer's Security Details in accordance with Clause 15.3(b) below; and

- e. Real-time fraud surveillance to enable the Bank to detect and block suspected fraudulent or unauthorised Transactions at any time in accordance with Clause 5.13 above.
- 11.11 The Bank shall have the absolute discretion from time to time to determine the scope of the Cyberbanking Service, set or change the daily Cut-Off Time, temporarily or permanently discontinue the operations of the Cyberbanking Service without notice or responsibility to the Customer.
- 11.12 The Bank is not liable for the consequences arising out of inaccurate or incorrect information supplied by the Customer.
- 11.13 The Bank shall not be liable for any damage to the Customer's computer terminal or Equipment or related facilities or any loss or corruption of the Customer's data in connection with the operation or use of the Cyberbanking Service. The Bank shall not in any event be liable for any indirect, special, incidental or consequential damages arising from or in connection with the provision of the Cyberbanking Service.

12 Disclosure of Information

- 12.1 The Customer shall consent and permit the Bank and each of its officers to divulge, reveal or disclose any and all customer information or deposit information (as defined in the Banking Act), particulars and information relating to the Customer, any credit facility, Account, Transaction or dealings between the Customer and the Bank, or any Transaction or use of any services by the Customer in connection with or to facilitate the use of the Cyberbanking Service, for any purpose whatsoever:
- a. within The Bank of East Asia Group (including its parent company, other branches or subsidiaries, affiliates and/or associates) or agents, which may be in Singapore or outside Singapore;
 - b. to the credit bureau as defined in the Banking Act for the purpose of assessing the Customer's credit worthiness or for any other purpose whatsoever as determined by the Bank;
 - c. to all government agencies and authorities in Singapore and elsewhere where such disclosure is required by law;
 - d. to any agents or contractors or third parties which have agreed to perform works or services (including any outsourced services) for the Bank ("Outsourced Service Providers/Subcontractors") which require the same for such purpose. The Customer hereby irrevocably and unconditionally authorises and consents to the Bank's disclosure of the Customer's information to its Outsourced Service Providers/Subcontractors, which may be in Singapore or outside Singapore, for the outsource of operational support services, IT support services, client-related support services and other functions in order to provide services to Customer or effecting or carrying out any transactions. The disclosure of Customer's information is to allow Outsourced Service Providers/Subcontractors to access, collect, copy, modify, store, process, dispose or use any Customer's information in order to provide the relevant outsourced relevant services;
 - e. to any person who provides or maintains any part of any system or Equipment relevant to the provision of any facility or Service to the Customer;
 - f. to any other person at any time:

- (i) which the Bank or any officer in good faith considers to be appropriate and in the interest of the Bank; or
- (ii) in connection with the use and maintenance of any Account or facility;
- g. to any person under a duty of confidentiality to the Bank and/or its affiliates;
- h. to any other financial institution or intermediary with which the Customer has dealings;
- i. to any assignee or transferee of the Bank or participant or sub-participant of the Bank's rights in relation to the Customer;
- j. to any other person as may be required in order for the Bank to comply with any applicable laws, regulatory requirements, orders of courts or tribunal, codes or guidelines and requests or requirements (whether or not having the force of law) of any competent government, quasi-government or regulatory, fiscal or monetary authority and other authorities, bodies or persons whether in Singapore or elsewhere;
- k. to the auditors and legal and other professional advisers of the Bank; or
- l. under the following circumstances:
 - (i) if such disclosure is required for the provision of services to the Customer; and/or
 - (ii) if such disclosure is required or requested by any relevant governmental or regulatory, agency, department or body, regardless of jurisdiction; and/or
 - (iii) if such disclosure is permitted pursuant to the Banking Act 1970 of Singapore or any other applicable law.

12.2 The Customer hereby consents to the collection, use and disclosure of their personal data by the Bank as set out in the Privacy Statement (Personal Data Protection Act) of BEA(S), as may be amended by the Bank from time to time.

12.3 To comply with legal or regulatory requirements as well as the requirements of the Bank's anti-money laundering measures, the Customer agrees that the Bank may, upon request, also transfer, share, exchange and disclose any data about the Customer, the underlying transactions and the Bank's comments on the Customer and its transactions to any payment recipients, beneficiaries, intermediaries, correspondent and agent banks, whether located in or outside Singapore, in relation to any inward or outward remittance or payment transactions received, effected or initiated by or on behalf of the Customer. The aforesaid data may include the Customer's identity, nature and place of business, transaction patterns and level of activities with the Bank, source of funds, nature of the remitting account, details of the ultimate beneficial owners, shareholders, group companies, officers and authorised signatories of the Customer, purpose and other details of the underlying transactions, counterparties, remittance and payments and onward fund movements and the supporting documents, relationship between the Customer and the other parties to the underlying transactions, as the aforesaid data are made available to the Bank.

13 Fees and Expenses

13.1 The Bank is entitled to levy fees and charges against the Customer to cover costs and expenses arising out of the running and operation of the Account and Services. The Bank reserves the right to revise all fees and charges from time to time with prior notice to the Customer.

14 Contacting the Bank via the Cyberbanking Service

14.1 The Customer may send the Bank and the Bank may send the Customer secure email messages via the 'Messages' function which is a secure function within the Cyberbanking Service.

- 14.2 The message function within the Cyberbanking Service shall only be used for routine communications where time is not of the essence. The message function, in particular, shall not be used for urgent or time-sensitive communications, nor for any of the following purposes:
- a. giving Instructions for Transactions;
 - b. giving personal information or updates of personal information;
 - c. reporting loss of cheques, PIN and other security matters.

The Bank shall not be responsible for any loss or damage arising from the Customer's failure to comply with the limitations stated herein for the use of the message function.

- 14.3 All messages to the Customer from the Bank shall be deemed delivered to the Customer from the time the message becomes retrievable, accessible or readable by the Customer whether or not it was in fact retrieved, accessed or read.

15 Terminating or Suspending Cyberbanking Services

- 15.1 The Bank reserves the absolute discretion at any time as it deems fit to modify, cancel, suspend or terminate i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service without giving reasons and without prior notice to the Customer. If i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service is cancelled, suspended or is not available for whatever reasons (whether or not within the control of the Bank), the Bank shall not be liable for any loss or damage suffered by the Customer in connection with such cancellation, suspension or unavailability.

- 15.2 Without prejudice to clause 15.1, the Customer acknowledges that the Bank shall be entitled to suspend or terminate the availability of the i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service immediately upon occurrence of any of the following events:
- a. there is any change of law which prohibits or renders illegal the maintenance or operation of i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service or any elements thereof;
 - b. the Customer commits any breach of or omits to observe any obligations under these Terms.

- 15.3 If the Customer becomes aware of any loss, misuse of Biometric Authentication, theft or unauthorised use of the designated mobile device(s) or reasonably believe or suspect that any other person knows or is making unauthorised use of the Customer's Security Details (e.g., to execute outgoing payment transactions, perform High-risk Activities etc.), the Customer undertakes to:
- a. Immediately activate the "Suspend Account" feature to disable and block access to the Customer's Cyberbanking Account(s), i-Token and Biometric Authentication on their online and mobile device(s); and
 - b. Immediately report such incident to the Bank. If the Customer is not able to report such incident to the Bank immediately or in any case no later than thirty (30) days from becoming aware of such incident, the Customer should provide the Bank with reasons for its delayed report. The Customer shall provide in its report all information reasonably requested by the Bank in relation to the incident, including but not limited to details of the affected Accounts, details of the incident (including the date and time of the incident), whether and what Security Details were used to perform the unauthorised activities, and any other information that may assist in investigating the unauthorised use or transaction. Upon receipt of such report from Customer, the Bank

is entitled to deny any subsequent access to BEA App, BEA Mobile Banking or Cyberbanking Service, or activation of i-Token, use of Biometric Authentication by the Customer and terminate the i-Token Service or Biometric Authentication for the Customer accordingly.

- 15.4 On the closure of the Account, the Cyberbanking Service for such Account shall be terminated. All outstanding, pending and scheduled Instructions submitted via the Cyberbanking Service for such Account shall be automatically cancelled upon closure of the Account.
- 15.5 The Customer can notify the Bank at any time, if the Customer no longer wishes to use the Cyberbanking Service, by writing to the Bank or attending in person at the Bank. If the Customer notifies the Bank by any other means, the Bank may ask the Customer to confirm this in writing. Any such termination of the Cyberbanking Service shall not affect the Customer's liabilities and obligations which have incurred or accrued and any Instruction provided to the Bank prior to such termination.
- 15.6 The Bank may suspend all or any part of the Cyberbanking Service in certain circumstances, including but not limited to the following:
 - a. to protect the security of the Cyberbanking Service or the Bank's systems; or
 - b. the Bank has reason to believe that there may have been (or there is likely to be) unauthorised or fraudulent use of the Cyberbanking Service.
- 15.7 The Bank may suspend the Customer's access to the Cyberbanking Service if the Customer does not log in for more than 6 months.
- 15.8 The Bank shall be entitled to close/terminate any or all the Cyberbanking Service immediately and without prior notice if:
 - a. there is any change of law which prohibits or renders the maintenance or operation of any Services or any part thereof illegal; or
 - b. the Customer commits any breach of or omits to observe any obligations under the Terms which, in the opinion of the Bank, amounts to a material default on the part of the Customer; or
 - c. the Bank's records show that the Customer has maintained no Accounts for such period as the Bank shall prescribe; or
 - d. the Bank determines, or has reason to believe that the Customer:
 - (i) has passed away; or
 - (ii) has become an undischarged bankrupt; or
 - (iii) has been convicted in Singapore or elsewhere of an offence for which the Customer has been found to have acted fraudulently, corruptly, or dishonestly.
- 15.9 The Bank shall act in accordance with the laws, rules, regulations, guidelines, requests, and/or recommendations of public and regulatory organisations or authorities operating in various jurisdictions, which relate to, amongst other things, the prevention of money laundering, terrorist financing, and the provision of financial and/or other services to any persons or entities which may be subject to sanctions. The Bank may take any action (including but not limited to the suspension or closure of the Account(s)) which it, in its sole and absolute discretion, considers appropriate to take in accordance with all such laws, rules, regulations, guidelines, requests, and/or recommendations. Such action may include, but is not limited to, the disclosure, interception, and/or investigation of any payment messages and other information or communications sent to or by the Customer or on the Customer's behalf through the systems of the Bank or any member of The Bank of East Asia Group; and making further enquiries as to whether a name which might refer to a sanctioned person or entity actually refers to that person or entity.

16 Limitations

- 16.1 The information contained on the Website and BEA App is provided by the Bank. Whilst the Bank uses reasonable endeavours to keep the information up to date and correct, the Bank makes no representations or warranties of any kind, expressed or implied, about (and accept no liability for) the completeness, accuracy, adequacy, security, timeliness, reliability, suitability or availability of any information contained on the Website and BEA App. The Bank expressly disclaims all liability and responsibility for any lack of completeness, accuracy, adequacy, security, timeliness, reliability, suitability or availability with respect to the information in the Website and BEA App. The Bank reserves the right to modify the content and/or the design of the Website and BEA App at any time without notice.
- 16.2 Any reliance which the Customer places on any information on the Website or BEA App is strictly at the Customer's own risk.
- 16.3 The Bank has used reasonable endeavours to ensure, as far as possible, that emails and Instructions sent via the internet are not subject to interference and remain secure and confidential. The Bank cannot, however, guarantee the absolute security of emails and Instructions sent via the internet. Messages and Instructions sent via the internet cannot be guaranteed to be completely secure as possible interception, loss or alteration may occur. We accept no responsibility for such occurrences or for any loss or damage that may arise as a result of such occurrences. By submitting Instructions and making use of the Cyberbanking Service, the Customer is deemed to acknowledge and accept this.
- 16.4 Save where the law requires, the Bank shall not be liable for any loss or damage, howsoever caused, including without limitation direct or indirect, special, incidental or consequential losses, damages or expenses arising or liability resulting from any failure, act or omission, error, interruption, defect, delay in operation or transmission, computer virus or system failure of the Customer's computer or software, or any internet browser provider, internet access provider, online service provider or by any agent or subcontractor for any of the foregoing.
- 16.5 Nothing on the Website or BEA App should be considered as providing financial advice. The Customer is recommended to consult the Customer's own independent financial advisor. In the event that you choose not to seek advice from your own independent financial advisor, you should consider whether the investment product (if any) is suitable for you. The Customer's eligibility for investment products and services offered by the Bank is subject to the determination and/or acceptance by the Bank. The investment products mentioned in the Website or BEA App are not necessarily obligations of the Bank or guaranteed by the Bank. All investments are subject to risks, including the possibility of loss of the initial sum invested.

17 Right of Waiver

- 17.1 No indulgence or concession granted by the Bank and no omission or delay on the part of the Bank in exercising any right, power or privilege hereunder shall operate as a waiver thereof, nor shall any single or partial exercise of any such right, power or privilege preclude any other or further exercise thereof or the exercise of any other right, power or privilege.

18 Severability

- 18.1 If any one or more provisions of the Terms, or any part thereof, shall be declared or adjudged to be illegal, invalid or unenforceable under any applicable law, such illegality or

unenforceability shall not vitiate any of the other provisions hereof which shall remain in full force, validity and effect.

19 Amendment

- 19.1 The Bank may revise any provisions contained in the Terms and/or introduce additional provisions at any time and from time to time after giving such reasonable notice as the Bank may reasonably determine. Such revisions and/or additions thereto shall become effective on a date specified by the Bank and shall be deemed to have been accepted by, and be binding on, the Customer if the Customer continues to use the Cyberbanking Services after such effective date.

20 Contracts (Rights of Third Parties) Act

- 20.1 A person who is not a party to these Terms shall have no right under the Contracts (Rights of Third Parties) Act 2001 to enforce any of its terms.

21 Complaints

- 21.1 Any complaint or dispute by the Customer in relation to the Bank's method of execution or provision of the Cyberbanking Service, its failure to execute the Customer's Instructions or in relation to any communications from the Bank or otherwise pursuant to the Terms shall be delivered in writing to the Bank's Liaison Officer at 60 Robinson Road, BEA Building, Singapore 068892 either within seven (7) Business Days of the delivery of the communication to the Customer or within the period of response specified by the Bank.
- 21.2 Where a complaint is received by the Bank pursuant to and in the time specified in clause 21.1 above, the Bank shall investigate such complaint and provide the Customer with a written response. The Customer shall co-operate with the Bank fully in any investigations made by the Bank or its appointees in discharge of its obligations made under this clause.
- 21.3 The Bank is a member of the Financial Industry Disputes Resolution Centre Ltd ("FIDREC"). In the event the Customer is not satisfied with the Bank's response, the Customer may file a complaint to the FIDREC.

22 General

- 22.1 The Customer acknowledges and confirms that the Customer has read, understood and agreed to be bound by the Terms before using the Cyberbanking Service. An additional copy of the Terms may be obtained by the Customer from the Bank's Website, the BEA App, at the Bank's branch or by calling the Cyberbanking Help Desk of the Bank.
- 22.2 The Terms are governed by and construed in accordance with the laws of Singapore. The courts of Singapore shall have exclusive jurisdiction to settle any dispute which may arise out of or in relation to the Terms, and the parties submit to such jurisdiction.
- 22.3 The Terms are only available in English. Words and phrases in the Terms shall be read and construed in accordance with the definitions contained hereto. Where the context permits, the singular includes the plural and vice versa, the masculine includes feminine and neuter and vice versa.