BEA東亞銀行

Terms and Conditions for Corporate Cyberbanking ~~Service~~and BEA Corporate Online Services

General Terms and Conditions for Corporate Cyberbanking and BEA Corporate Online Services
Schedule I Terms and Conditions for Bank Services relating to Faster Payment System
Schedule II Terms and Conditions for i-Token Service and Biometric Authentication
Schedule III Terms and Conditions for Open Application Programming Interface Service and Third Party Service Provider Consent Management Service

In consideration of The Bank of East Asia, Limited (the "Bank") agreeing to open and continue to maintain Corporate Cyberbanking or BEA Corporate Online account(s) and/or provide its services, I/we (the "Customer") hereby understand and agree that the following terms and conditions and the Schedule(s) (as amended from time to time) (collectively referred to as the "Terms") shall apply to the accounts and the ~~services~~Systems provided by the Bank and shall be binding on the Customer.

General Terms and Conditions

Corporate Cyberbanking and BEA Corporate Online is provided by the Bank to the Customer on the following terms and conditions~~-~~:

1. Definitions

The following words and expressions shall have the following meanings:-

Administrator:	With respect to Corporate Cyberbanking, any person designated by any Authorised Person to administer the System (including the creation of the 'Normal User' (including the username and PIN) and, registration of services to be used by each Normal User and Signer via the System, the designation of the 'Normal User' as a 'Signer' and the class to which the Signer belongs under the System and to register and subscribe for i-Token Service for the Signer. With respect to BEA Corporate Online, any person designated by any Authorised Person to assist any Authorised Person to create the user profile of the users of the System, to register and subscribe for i-Token service for any user and to register the services to be used via the System. "Administrator" is sometimes called "System Administrator" in BEA Corporate Online.
Associated Account:	An account maintained with the Associated Institution and nominated by the parent company, subsidiary or associate of the Customer, according to such procedures as the Bank may prescribe from time to time, for the operation with full rights and power (unless expressly restricted by the parent company, subsidiary or associate of the Customer in writing to the

Bank) by the Customer or by the Customer's authorised person or agent in the System.

Authorisation Matrix: An account maintained withA matrix indicates the Associated Institutionauthorisation classes, and nominatedthe class or combination of classes required for approving different transaction values within the limit as prescribed by the Customer, according to such procedures as the Bank may prescribe from time to time. "Authorisation Matrix" is sometimes called "Signing Arrangement" in BEA Corporate Online., to receive the Corporate Cyberbanking and/or subsequently accepted by the Bank from time to time to receive the Corporate Cyberbanking.

Related Account:

Authorisation Matrix:

Associated Institution: Any branch of the Bank or any company which is a subsidiary or an associate of the Bank (or any branch thereof).

Customer: Any entity, sole proprietorship, partnership or corporation who applies for the Corporate Cyberbanking (which shall include its representative and lawful successor (as the case may be)).

Corporate Cyberbanking: An electronic banking services system which allows the Customer inter alia to gain access to financial information or information in respect of the Customer's Related Account(s) and Associated Account(s) maintained with the Associated Institution and to carry out certain banking functions (as prescribed by the Bank from time to time) in the nominated account(s).

PIN: Any personal identification number ("PIN") issued to the Customer (or any of the Customer's representatives) including the PIN(s) for Administrator(s) and the PIN(s) for Signer(s) and any PIN adopted by the Customer (or any of the Customer's representatives) which may be used to access the Corporate Cyberbanking.

Associated Account: An account maintained with the Associated Institution and nominated by the subsidiary or associate of the Customer, according to such procedures as the Bank may prescribe from time to time, for the operation with full rights and power (unless expressly restricted by the subsidiary or associate of the Customer in writing to the Bank) by the Customer or by the Customer's authorised person or agent in the Corporate Cyberbanking and /or subsequently accepted by the Bank from time to time.

Authorised Person:	Any person designated and appointed by the Customer to act on behalf of the Customer and to be responsible for the management and control of the use of the ~~Corporate Cyberbanking~~System (including the appointment of users) by the Customer (as described in paragraph 2.3 hereinafter).
~~Administrator:~~	~~Any person designated and appointed by the Authorised Person to administer the Corporate Cyberbanking as well as to create the 'Normal User' (including the username and PIN) and to link the 'Normal User' to be 'Signer' under the Corporate Cyberbanking.~~
~~Normal User:~~	~~Any person designated and appointed by the Administrator to use the Corporate Cyberbanking but is not allowed to approve transactions under the Corporate Cyberbanking.~~
~~Signer:~~	~~Any person designated and appointed by the Administrator to use the Corporate Cyberbanking and allowed to approve transactions, according to the Authorisation Matrix given to the Bank and within the limit as prescribed by the Bank from time to time, by using PIN(s) provided by the Bank or other valid means acceptable to the Bank (including Digital Certificate) under the Corporate Cyberbanking.~~
~~Authorisation Matrix:~~	~~A matrix indicates the authorisation classes, and the class or combination of classes required for approving different transaction values within the limit as prescribed by the Bank from time to time.~~
~~Digital Certificate:~~	~~Any certificate issued by a certification authority (as defined in the Electronic Transactions Ordinance (Cap 553)) that the Bank has accepted for use in a transaction through the Corporate Cyberbanking.~~
~~Digital Signature:~~	~~In relation to an electronic record, means an electronic signature of the signer (as defined in the Electronic Transactions Ordinance (Cap 553)).~~
~~Instruction:~~ Customer:	Any entity, sole proprietorship, partnership or corporation who applies ~~Any request or instruction given by the Customer or any user (which in the context hereinafter includes without limiting to (as the case may be) the Authorised Person, Administrator, Normal User and Signer for and on behalf of the Customer) to the Bank effected through the Corporate Cyberbanking by use of a PIN or other valid means which comply with all the standards and procedures that the Bank may from time to time require including a Digital Signature created from a Digital Certificate.~~ for the System (which shall include its representative and lawful successor (as the case may be)).
i-Token Service	As defined in the Bank's Terms and Conditions for i-Token Service and Biometric Authentication (as amended from time to time).

Instruction:	Any request or instruction given by, or purports to be given by, the Customer or any user (which in the context hereinafter includes without limiting to (as the case may be) the Authorised Person, Administrator, Normal User and Signer for and on behalf of the Customer) to the Bank through the Corporate Cyberbanking or BEA Corporate Online by use of a PIN, (where applicable) a security code generated or designated by the i-Token Service or other valid means in accordance with the Authorisation Matrix and which comply with all the standards and procedures that the Bank may from time to time require.
Normal User:	With respect to Corporate Cyberbanking, any person designated by any Administrator to create and send details of proposed transactions to the Bank via the System but who is not allowed to approve transactions under the System. With respect to BEA Corporate Online, any person designated by an Authorised Person to view and/or create and send details of proposed transactions to the Bank via the System, but who does not have the authority to approve transactions. "Normal User" is sometimes called "Viewer" or "Maker" in BEA Corporate Online.
PIN:	Any personal identification number ("PIN") issued to the Customer (or any of the Customer's representatives) including the PIN(s) for Administrator(s) and the PIN(s) for Signer(s) and any PIN adopted by the Customer (or any of the Customer's representatives) which may be used to access the System.
Related Account:	An account maintained with the Associated Institution and nominated by the Customer, according to such procedures as the Bank may prescribe from time to time, to receive the services under the System.
Signer:	With respect to Corporate Cyberbanking, any person designated and appointed by any Administrator to use the System and who is allowed to approve transactions according to the Authorisation Matrix given to the Bank and within the limit as prescribed by the Bank from time to time, by using PIN(s) provided by the Bank or other valid means acceptable to the Bank under the System. With respect to BEA Corporate Online, any person designated by any Authorised Person to use the System who is allowed to approve financial transactions which involve fund transfers and such other types of transactions as may be designated by the Bank from time to time according to the Authorisation Matrix given to the Bank and within the limit

as prescribed by the Bank from time to time, by using PIN(s) provided by the Bank or other valid means acceptable to the Bank under the System. "Signer" is sometimes called "Approver" in BEA Corporate Online. Each Authorised Person shall be deemed to be an ~~Signer~~ Approver.

System: An electronic banking services system which allows the Customer inter alia to gain access to financial information or information in respect of the Customer's Related Account(s) and Associated Account(s) maintained with the Associated Institution and to carry out certain banking functions and transactions (as prescribed by the Bank from time to time) in the nominated account(s), currently under the names Corporate Cyberbanking and BEA Corporate Online respectively.

Third Party Account A deposit account with any bank held by a party other than the Customer.

2. Use of Service

2.1 The Bank may grant to the Customer the facility to carry out certain banking functions in the account(s) through internet or other electronic delivery channels subject always to the Rules and Regulations / Terms and Conditions governing such account(s) as prescribed by the Bank from time to time.

2.2 Either party may suspend or terminate ~~this Corporate Cyberbanking~~the System on thirty days' notice to the other provided that the Bank shall be entitled to suspend or terminate ~~this Corporate Cyberbanking~~the System immediately and without prior notice in the event of a ~~material~~ breach (as shall be determined by the Bank) of ~~it~~these Terms and Conditions by the Customer ~~or~~, upon closure of the Customer's account(s) with the Bank or in exceptional circumstances.

2.3 The Customer shall designate and appoint one or more than one Authorised Person(s) to give instructions relating to the access and use of the ~~Corporate Cyberbanking~~System to the Bank on behalf of the Customer. The instructions given by any one of the Authorised Person(s) shall be binding upon the Customer. The Authorised Person(s) shall manage and control the access of and the use of the ~~Corporate Cyberbanking~~System including PIN management pursuant to the terms and conditions and all other terms governing or relating to ~~Corporate Cyberbanking~~the System as prescribed by the Bank from time to time and the addition and deletion of Related Accounts, Associated Accounts and pre-designated Third Party Accounts and the increase of daily transaction limits.

2.4 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. Without prejudice to the generality

of Clause 2.2 of these Terms and Conditions herein, the Bank may take any action (including but not limited to the suspension or termination of the System and suspension or closure of the account(s) of the Customer) 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 BEA 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.

3. PIN

3.1 The Customer shall nominate one or more individual(s) (including, where the Customer is a sole-proprietorship, the sole proprietor) to use and ~~collect~~receive the PIN(s) for ~~Corporate Cyberbanking~~the System. Upon receipt of the PIN(s) by the Customer, its authorised person, staff, servant or employee, the PIN(s) shall be kept by the Customer at its own sole risk and the Customer shall be fully liable and responsible for any loss, claim, damage and cost whatsoever arising from or in connection with any negligence, improper use, misuse, theft or loss of the PIN(s) and shall keep the Bank fully indemnified in respect thereof, notwithstanding that the authorised person, staff, servant or employee has not signed the acknowledgement letter.

3.2 The Customer and any user including but not limited to the Authorised Person, Administrator, Normal User and Signer shall act in good faith, exercise reasonable care and diligence in keeping the PIN(s) strictly confidential at all times and agrees to be fully responsible for any accidental, unintentional or unauthorised disclosure of the PIN(s) to any other person and shall be wholly responsible for any direct and indirect losses and/or liabilities caused by or in connection with the unauthorised use of such PIN(s).

3.3 The Customer or any user including but not limited to the Authorised Person, Administrator, Normal User and Signer shall not use personal secret code such as identity card number, telephone number, etc., or popular number sequences, or recognisable part of the Customer / user's name when setting PIN for ~~Corporate Cyberbanking and password(s) for Digital Certificate(s).~~the System.

3.4 ~~-~~The Customer or any user including but not limited to the Authorised Person, Administrator, Normal User and Signer shall avoid using the same PIN or password, or user identification for accessing other services (e.g. accessing other web sites).

3.5 The Customer undertakes to notify the Bank immediately in writing in the event of any suspicion or the Customer ought to have come to any reasonable suspicion relating to the unauthorised disclosure or use of the PIN(s).

3.6 Notwithstanding Clause 3.2 above, the Customer agrees to indemnify the Bank against any action, liability, proceedings, cost and expenses on a full indemnify basis (including

legal fees) suffered by the Bank which is directly or indirectly related to the use of the ~~Corporate Cyberbanking~~System by the Customer as a result of or incidental to the negligence or failure of the Customer to comply with any of the terms and conditions contained herein, the service guides and/or user guides in respect to Corporate Cyberbanking ~~and other terms and conditions governing or relating to Corporate Cyberbanking as prescribed by the Bank from time to~~ time. .

3.7 The Customer or Authorised Person may request, in writing or via the ~~Corporate Cyberbanking~~System, the alteration of the PIN if necessary from time to time. For the purpose of these ~~conditions~~Terms and Conditions, the term PIN shall be the PIN currently in use.

3.8 The issuance or selection of a new PIN shall not be construed as the commencement / creation of a new contract.

4. Instruction

4.1 All transactions entered into pursuant to the ~~instructions~~Instructions given to the Bank via the ~~Corporate Cyberbanking~~System shall be subject to the terms and conditions governing such transactions as prescribed by the Bank from time to time.

4.2 The Customer agrees to pay the Bank's scale of charges for the provision of ~~Corporate Cyberbanking~~the System as advised to the Customer by the Bank. The Bank may at any time without giving notice to or obtaining consent from the Customer set-off or transfer any monies standing to the credit of any of the Customer's accounts of whatsoever description (including but not limited to current, savings, fixed or call deposit account(s)) at any Associated Institution towards the discharge of all sums due to the Bank or arising out of the use of the ~~Corporate Cyberbanking.~~System.

4.3 The Customer shall be fully responsible for all Instructions and agrees to pay any normal bank charges associated with the Instructions. In the event that the Customer fails to complete an agreed or confirmed foreign exchange contract due to insufficient funds or unauthorised overdrawing in the account as designated in the Customer Instruction or otherwise, the Bank shall be entitled to set off the said foreign exchange contract at the prevailing exchange rate and to charge the Customer for any difference in the exchange thus arising.

4.4 In addition to Clause 4.9, the Bank shall be at its own discretion entitled but not obliged to accept Instructions~~which have been properly authorised by the Customer~~, particularly if such instructions conflict or may conflict with or are in any way inconsistent with any other instructions received under any other mandate given by the Customer to the Associated Institution whether or not relating to any of the Customer's Related Accounts. 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.

4.5 ~~Under~~Subject to the provisions of these Terms and Conditions, the Bank is authorised to act on the Instructions and all transactions (including the transactions of the Customer's Related Account(s), the Third Party Account(s) and the Customer's Associated Account(s)) effected by the Bank pursuant to Instructions received by the Bank ~~from the Customer or any user through the Corporate Cyberbanking, and in conjunction with the Digital Signature created from the Customer's or any user's Digital Certificate~~ shall be binding on the Customer and any user in all respects.

4.6 If the Customer's Related Account is maintained in joint names, then each and every one of the Related Account holders shall be jointly and severally liable for all transactions involving the use of the ~~Corporate Cyberbanking~~System and these Terms and Conditions shall apply to each of the Related Account holders separately and jointly.

4.7 The Customer's Associated Account holder and the Customer shall be jointly and severally liable for all transactions of the Customer's Associated Account involving the use of the ~~Corporate Cyberbanking~~System and these Terms and Conditions shall apply to each of the Associated Account holders separately and jointly.

4.8 All Instructions, once given, shall be irrevocable and binding on the Customer or any user. The Bank's record of Instructions and transactions shall be conclusive evidence against the Customer or any user.

4.9 Any Instruction given to the Bank via the ~~Corporate Cyberbanking~~System shall operate as a request by the Customer to the Bank to act on the Instruction provided that the Bank may, but shall not be obliged to, act on any such Instruction which would result in a Related Account or Associated Account becoming overdrawn ~~without authorisation~~ or if the Related Account or Associated Account is on hold, or frozen or dormant or in any other circumstances which the Bank may in its sole judgment consider appropriate. Any Instruction, once given, may not be withdrawn by the Customer without the written consent of the Bank. All Instructions which are understood and acted on by the Bank in good faith, shall be binding on the Customer. The Bank shall be under no duty to inquire into the authenticity of any Instructions or the identity or authority of the person giving or purporting to give any Instructions. The Bank may treat all Instructions given as fully authorised and binding on the Customer regardless of the circumstances prevailing at the time of the Instructions being 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 he is under an express duty to the Bank to prevent any fraudulent, forged or unauthorised Instructions being given.

4.10 The Customer hereby appoints the Bank as the Customer's agent for the purpose of:

(a) instructing on the Customer's behalf any relevant Associated Institution to transmit or otherwise communicate to the Bank and/or the ~~Corporate Cyberbanking~~System any information concerning the Customer and the Customer's account(s) (whether now in existence or will be opened afterwards) with any such Associated Institution, as well as the Customer's Associated Account(s) under the ~~Corporate Cyberbanking~~System; and

(b) opening, continuing and conducting accounts with any Associated Institution in order to give effect to any Customer Instruction, and the Customer agrees that any such account will be opened and conducted on such terms and conditions as that Associated Institution shall reasonably consider appropriate.

4.11 The Customer acknowledges that a copy of the Notice relating to the Personal Data (Privacy) Ordinance has been provided by the Bank for the Customer's perusal and understanding~~.~~ and the Customer agrees with the terms of the same (as the same may be amended from time to time).

4.12 The Customer authorises the Bank to provide third parties with such information relating to the Customer, the Customer's Related Account(s), and the Customer's Associated Account(s) as may, in the Bank's reasonable opinion, be necessary in order to give effect to an Instruction or in order to comply with the order of any court, government agency tribunal or lawful authority in any jurisdiction or any applicable legal requirement, guidelines, codes which the Bank deems necessary.

4.13 The Customer acknowledges that information concerning the Customer, the Customer's Related Account(s) and the Customer's Associated Account(s) may be transmitted to or through and/or stored in various countries or states. The Customer authorises such transmission and/or storage as the Bank or any Associated Institution shall reasonably consider necessary or appropriate in the provision of the ~~Corporate Cyberbanking~~System.

4.14 The Bank shall endeavour to take all steps as far as reasonably practicable to ensure that information made available by the ~~Corporate Cyberbanking~~System is correct and updated at regular intervals. The transaction details and account balances as shown in the Customer's terminal or any print-out are for reference only. Those transaction details and account balances as recorded in the Bank's system will be conclusive. The Customer agrees and confirms that the Bank shall not be held liable for or in connection with the accuracy of all or any of the information received by the Customer via the ~~Corporate Cyberbanking.~~System.

4.15 Transactions involving any transfer of funds between accounts (including the Related Accounts and Associated Accounts) on any day may at the Bank's sole discretion be processed to the said accounts concerning the transfer of funds on the day of the transaction or failing that, on the next banking day.

~~4.16~~ The amounts which the Customer shall be entitled to transfer via the ~~Corporate~~
~~4.17~~4.16 ~~Cyberbanking~~System shall be limited to the individual limit and the aggregate daily limits of Hong Kong Dollars 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 ~~Corporate Cyberbanking~~System or for any other reason(s).

~~4.18~~4.17 The Customer can use the ~~Corporate Cyberbanking~~System for transfer/payment transactions only if there are sufficient funds in the respective Related Account(s) or Associated Account(s~~).~~) or pre-arranged credit.

4.194.18 The Customer irrevocably authorises the Bank to debit the Related Account(s) or Associated Account(s) with the amount of any transfer or withdrawal from such account effected via the ~~Corporate Cyberbanking~~System.

4.19 (*applicable to BEA Corporate Online only*) The Customer understands and agrees that the one-time password (OTP) for verifying transactions through the System will be sent by short message service ("SMS") to the mobile phone number registered by the Customer for such purpose or, if no such number has been registered, to the last known mobile phone number of the Customer in the record of the Bank.

5. Limitation of Liability

5.1 The Customer agrees that the Bank shall not be liable to the Customer for any failure to provide the ~~Corporate Cyberbanking~~System which is attributable (whether wholly or partially) to any cause beyond the Bank's control including but not limited to any equipment malfunction or failure and delay or failure of any third party communication systems.

5.2 Under no circumstances shall the Bank be liable to the Customer (whether in contract, tort, including negligence, strict liability or otherwise) for any indirect or consequential loss (whether foreseeable by the Bank or not) arising out of or related to the Customer's use of the ~~Corporate Cyberbanking~~System and the Bank shall not be liable for any damage to the Customer's terminal or related facilities or any loss or corruption of the Customer's data in connection with the operation of the ~~Corporate Cyberbanking~~System.

5.3 Subject to the provisions herein, the Bank's liability (if any) to the Customer in relation to the provision of the ~~Corporate Cyberbanking~~System shall only be limited to the amount of the relevant transaction or the direct damages sustained, whichever is less. The Bank shall in no circumstances be liable to the Customer for any indirect, special or consequential loss or damages.

5.4 Subject to the provisions hereof and only in the absence of negligence on the part of the Customer or any of its users under the ~~Corporate Cyberbanking~~System, the Customer shall not be liable for any unauthorised transaction performed through the internet due to :

(a) a computer crime not prevented by the security system of the Bank; or
(b) a human or system error caused by the Bank, resulting in an improper transaction, leading to the lost or misplaced funds; or
(c) a missed or mis-directed payment caused by the Bank.

The Customer shall be entitled to reimbursement from the Bank for interest or late penalties incurred by the Customer for missed payments directly attributable to the foregoing causes (a), (b) and (c).

5.5 The Customer agrees that the Bank shall not be liable for any losses due to ~~nonnotification~~non-notification by the Customer when facilities such as a telephone hot-line are made available by the Bank unless such facilities are not made available by the

Bank during particular periods, provided that the Customer notifies the Bank within a reasonable time after the facilities have become available again.

6. Warranties

6.1 The Customer shall (and shall procure and ensure each Authorised Person, Administrator, Signer and Normal User shall) ensure that security measures within the Customer's control are at all times both adequate and properly maintained and understands and agrees that the failure on the part of the Customer to comply with any one of the security precautionary measures set out in the Important Notes for Security in relation to Cyberbanking and any Advice on Security Tips as prescribed by the Bank from time to time may lead to security breach and the Bank shall not in any event be held liable for any loss or damage suffered by the Customer as a result thereof. If the Customer fails to ~~do~~comply with, or to procure the Authorised Person, Administrator, Signer or Normal User to ~~do~~comply with, the security precautionary measures, the Customer shall be liable for all unauthorised Transactions and all direct and indirect losses or damages. The Bank may at all times and from time to time in its sole discretion to update the security precautionary measures as set out in the Important Notes for Security in relation to Cyberbanking and any Advice on Security Tips without prior notice.

6.2 The Customer understands ~~Corporate Cyberbanking's~~the System's Security Control features as set out in the Important Notes for Security in relation to Cyberbanking and any Advice on Security Tips as prescribed by the Bank from time to time. The Customer also understands and warrants to exercise due care and good internal control within the Customer's operations from time to time and to use its best efforts to implement segregation of duties among Authorised Persons, Administrators, Signers and Normal Users when using ~~Corporate Cyberbanking.~~the System. The Bank shall be under no obligation to investigate or verify the authority of any person effecting Customer Instructions.

6.3 The Customer (sole proprietorship or partnership firm), and the proprietor or partners and persons carrying on business in the name of the Customer now or at any time hereafter shall be jointly and severally liable under these Terms and Conditions.

6.4 The Customer (sole proprietorship or partnership firm) shall advise the Bank of any change in its constitution or membership and unless expressly released by the Bank or under any applicable law, the Customer and all persons signing the ~~Application~~application form for ~~Corporate Cyberbanking~~use of the System as the proprietor or partners of the Customer shall continue to be liable hereunder irrespective of any change.
~~be liable hereunder irrespective of any change.~~

6.5 The Customer (Limited Company or Association) has been duly incorporated or formed and is in good standing.

6.6 The Customer warrants and represents that all acts, conditions, things required to be done, performed and observed in order that these Terms and Conditions shall constitute the

legal, valid and binding obligations of the Customer enforceable in accordance with its terms have been done, performed and observed in strict compliance with all applicable laws and Articles of Association or other constitutional documents of the Customer. ~~applicable laws and Articles of Association or other constitutional documents of the Customer.~~

~~7.~~

6.7 The Customer warrants to the Bank that (a) neither itself nor any user of the System will give any Instruction to the Bank in any country or jurisdiction where the offering of any of the services under the System is unlawful; (b) neither itself nor any of the users of the System will or will attempt to, reverse engineer, decompose, disassemble or otherwise tamper with any software relating to the System; (c) each of the Customer and the users of the System will ensure that the browser cache memory will be cleared as soon as it signs off each time after having given an Instruction through use of computer and it will exit the browser immediately after having given all its Instructions through use of computer.

7. Others

7.1 The granting of access to the ~~Corporate Cyberbanking~~ System shall be at the sole discretion of the Bank and the Bank has the full right to cancel or suspend the ~~Corporate Cyberbanking~~System or any element thereof at any time. In particular, the Customer understands that the Bank may terminate the services of the Corporate Cyberbanking by giving prior notice to the Customer and replace it with the BEA Corporate Online, and the roles and powers of the Administrator and the Authorised Person under the BEA Corporate Online would be different from those under the Corporate Cyberbanking. The Customer has been advised to familiarize itself of the respective roles and powers of the Administrator and the Authorised Person under the BEA Corporate Online as stated in these Terms and Conditions and take such action and make such adjustments as it deems appropriate as soon as it has received a notice from the Bank regarding the replacement of the Corporate Cyberbanking.

7.2 Without prejudice to the generality of Clause 7.1, the Bank shall be entitled to terminate immediately the ~~Corporate Cyberbanking~~System provided to the Customer if :

(a) there is any change of law which prohibits or renders illegal the maintenance or operation of such ~~Corporate Cyberbanking~~System or any elements thereof;

(b) the Customer shall commit any breach of or omit to observe any obligations under these Terms and Conditions which, in the sole opinion of the Bank, amounts to a material breach or default on the part of the Customer; or

(c) the Bank's records show that the Customer has maintained no Related Account and Associated Account for such period as the Bank shall prescribe from time to time.

7.3 The Customer shall only be entitled to obtain access to the ~~Corporate Cyberbanking~~System during the ~~Corporate Cyberbanking~~operating hours of the System specified by the Bank from time to time.

7.4 The Bank shall have the absolute discretion from time to time to determine the scope of the ~~Corporate Cyberbanking~~System, set or change the daily cut-off time, withdraw or discontinue the operations of ~~Corporate Cyberbanking~~System without notice or responsibility to the Customer. Any transactions performed through the ~~Corporate Cyberbanking~~System after the daily cut-off time shall be treated as next business day value transactions. Since the ~~Corporate Cyberbanking system~~System may be accessed from any country, the daily cut-off time in Hong Kong shall prevail.

7.5 The cost and expense to obtain and maintain suitable equipment to access the System shall be borne by the Customer.
~~Corporate Cyberbanking shall be borne by the Customer.~~

~~7.6~~ The Bank will not assume any responsibility or obligation for any transaction or error ~~7.7~~7.6 arising out of failure of the Customer to provide or input sufficient or accurate data to enable the said transaction to be effected through ~~Corporate Cyberbanking~~the System.

~~7.8~~ The Customer understands and acknowledges that ~~Corporate Cyberbanking~~the System is provided as an additional service in relation to banking transactions with the Bank and shall not be considered as a substitute for other method(s) of effecting banking transactions. In the event that ~~Corporate Cyberbanking~~the System is terminated by the Bank or not available for
any reason whatsoever (whether or not within the control of the Bank), the Customer ~~7.9~~7.7 shall have no claim whatsoever against the Bank and shall use other available means to effect banking transactions.

~~7.10~~ The Customer shall forthwith notify the Bank in writing of any change of address or other pertinent information and the Bank is entitled to rely on and treat the information in the Bank's records as true and accurate until the Bank receives such written notification of ~~7.11~~7.8change from the Customer. All communications will be deemed to have been delivered to the Customer at the time of delivery.~~.~~

~~7.12~~7.9 These Terms and Conditions shall be governed by the applicable laws of The Hong Kong Special Administrative Region and by the Bank's by-laws, regulations and practices, brought to the attention of the Customer by display, advertisement or otherwise as the foregoing are now in effect or as hereafter amended, enacted or adopted. The Courts of Hong Kong shall have the non-exclusive jurisdiction to determine, enforce and adjudicate all disputes and claims arising out of the above and in connection therewith.

~~7.13~~7.10 The Bank may revise any of the terms or add new terms to these Terms and Conditions
at any time. The revised terms and conditions when displayed, advertised or brought to the attention of the Customer by appropriate means shall become effective and be binding on the Customer and if the Customer continues to maintain the ~~Corporate Cyberbanking~~System after the effective date thereof, such revisions will be deemed to be accepted.

~~7.14~~7.11 These Terms and Conditions are additional to, and not in substitution for, any other terms and conditions relating to the conduct of the Customer's Related Account(s) and the Customer's Associated Account(s) with the Associated Institution. If at any time any of these terms and conditions becomes invalid or unenforceable, such shall not affect the validity and/or enforceability of any of the other terms and conditions hereof.

~~7.15~~7.12 The Chinese version of these Terms and Conditions is for reference only. If there is any conflict between the English and the Chinese versions, the English version shall prevail.

~~7.16~~7.13 Where the context permits, the singular includes the plural and vice versa, the masculine includes feminine and neuter and vice versa.

~~7.17~~7.14 These Terms and Conditions shall be binding on and enure to the benefit of the Bank and the Customer and the respective successors and assigns of the Bank and the Customer.

~~7.18~~7.15 No person other than the Customer or the Bank will have any right under the Contracts (Rights of Third Parties) Ordinance (Cap. ~~623 of the Laws of Hong Kong) to enforce or~~623 of the Laws of Hong Kong) to enforce or enjoy the benefit of any of the provisions of these Terms and Conditions, save that each Associated Institution may enforce and enjoy the benefits of these Terms and Conditions. Notwithstanding anything contained in these Terms and Conditions, the consent of any person (including the Customer and the Associated Institutions) is not required for the termination or amendment of these Terms and Conditions.
~~enjoy the benefit of any of the provisions of these Terms and Conditions.~~

8. Special Terms and Conditions

8.1 The use of the services provided by the Bank to the Customer to facilitate payments and funds ~~————~~transfers using the Faster Payment System is subject to the ~~provisions of~~Terms and Conditions for Bank Services relating to Faster Payment System as set out in Schedule I~~.~~ (as the same may be amended from time to time).

8.2 The use of the i-Token Service and Biometric Application for Mobile App provided by the Bank is subject to the Terms and Conditions for i-Token Service Biometric Application for Mobile App as set out in Schedule II (as the same may be amended from time to time).

8.3 The use of the Open Application Programming Interface Service and the Third Party Service Provider Consent Management Service provided by the Bank is subject to the Terms and Conditions for Open Application Programming Interface Service and the Third Party Service Provider Consent Management Service as set out in Schedule III (as the same may be amended from time to time).

Schedule I Terms and Conditions for Bank Services relating to Faster Payment System

1. ~~1.~~ Bank Services relating to Faster Payment System

~~(a)~~ We provide the Bank Services to customers to facilitate payments and funds transfers using the Faster Payment System. The Faster Payment System is provided and operated by HKICL. The Bank Services are therefore subject to the rules, guidelines and procedures imposed by HKICL in relation to the Faster Payment System from time to time. These Terms and Conditions govern our provision to you and your use of the Bank Services. The Bank Services form part of our banking services. These Terms and

~~(b)~~(a) Conditions supplement and form part of the Terms and Conditions for Corporate Cyberbanking ~~Terms~~ and ~~Conditions~~BEA Corporate Online Services (the "Existing Terms"). The provisions of the Existing Terms (other than the provisions of this Schedule I) continue to apply to the Bank Services to the extent that they are relevant and not inconsistent with the provisions in these Terms and Conditions. Unless otherwise specified, the provisions of these Terms and Conditions prevail if there is any inconsistency between them and the other provisions of the Existing Terms with respect to the Bank Services.

~~(c)~~(b) By requesting us to register any Proxy ID for you in the HKICL FPS or to set up any eDDA for you using the HKICL FPS, or by initiating any payment or funds transfer using the HKICL FPS, you will be regarded as having accepted and will be bound by the provisions of these Terms and Conditions. You should not request us to register any Proxy ID or set up any eDDA for you and should not initiate any payment or funds transfer using the HKICL FPS unless you accept the provisions of these Terms and Conditions.

~~(d)~~(c) In these Terms and Conditions, the following terms have the following meanings:

"Addressing Service" means a service provided by HKICL as part of HKICL FPS to facilitate customers of Participants to use predefined Proxy ID instead of account number to identify the destination of a payment or funds transfer instruction and other communications for the purpose of HKICL FPS.

"Bank Services" means the services provided by us to customers from time to time to facilitate payments and funds transfers using HKICL FPS and the Addressing Service, eDDA Service and any other services and facilities provided by HKICL in connection with the Faster Payment System from time to time.

"Default Account" means the account maintained by you with us or any other Participant and set as the default account for receiving payment or funds using HKICL FPS or (if and to the extent specified or permitted by the rules, guidelines and procedures of HKICL) for debiting payment or funds using HKICL FPS.

"eDDA" means a direct debit authorisation set up by electronic means using HKICL FPS.

"eDDA Service" means a service provided by HKICL as part of HKICL FPS to facilitate customers of Participants to set up direct debit authorisation.

"Faster Payment System Identifier" or **"FPS ID"** means a unique random number generated by HKICL FPS to be associated with the account of a customer of a Participant.

"HKICL" means Hong Kong Interbank Clearing Limited and its successors and assigns.

"HKICL FPS" or **"Faster Payment System"** means the Faster Payment System and related facilities and services provided, managed and operated by HKICL from time to time for (i) processing direct debits and credits, funds transfers and other payment transactions and (ii) exchanging and processing instructions relating to eDDA Service and Addressing Service.

"Hong Kong" means the Hong Kong Special Administrative Region of the People's Republic of China.

"Participant" means a participant of HKICL FPS which may be a bank or other financial institution, a retail payment system operator, a licensed stored value facility, or any other person accepted by HKICL as a participant of HKICL FPS from time to time.

"Proxy ID" means the identifiers which may be accepted by HKICL for registration in the Addressing Service to identify the account of a customer of a Participant, including the mobile phone number or email address of the customer, or the FPS ID.

"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 HKICL, we or any other Participant or the respective affiliates or group companies, or you are subject or are expected to comply with from time to time.

"you" and **"your"** means each customer to whom we provide Bank Services and, where the context permits, includes any person authorised by the customer to give instructions or requests to us in connection with the use of the Bank Services.

"we", **"us"** and **"our"** means The Bank of East Asia, Limited and its successors and assigns.

2. Scope of Bank Services and conditions for use

(a) We provide the Bank Services to customers to facilitate payment and funds transfer using the Faster Payment System and the Addressing Service, eDDA Service and any other services and facilities provided by HKICL in connection with the Faster Payment System from time to time. We have the right to set or vary from time to time the scope of the Bank Services and the conditions and procedures for using the Bank Services. In order to use the Bank Services, you have to accept and follow these conditions and procedures.

(b) We may provide the Bank Services to facilitate payment and funds transfer in any currency specified by us from time to time, including Hong Kong dollars and Renminbi.

(c) In order to enable us to handle an instruction for you in relation to payment or funds transfer using HKICL FPS, you have to provide or input the necessary information and complete the process by such means or in such manner prescribed by us from time to time.

(d) All payment or funds transfer transactions using HKICL FPS will be processed, cleared and settled under the interbank clearing and settlement arrangements including without limitation the arrangements in relation to the Faster Payment System agreed by the Participants and HKICL from time to time.

(e) We reserve the right to suspend or terminate the Bank Services in whole or in part at any time without giving notice or reason.

3. Addressing Service - registration and amendment of Proxy ID and related records

(a) In order to use the Addressing Service to receive payment or funds transfer using HKICL FPS, you have to register your Proxy ID in the HKICL FPS. We have discretion as to whether to offer the FPS ID as Proxy ID to you.

(b) Registration and amendment of Proxy ID and related records in the HKICL FPS must be done in accordance with the applicable rules, guidelines and procedures imposed by HKICL from time to time. In order to enable us to register or amend Proxy ID or any related records for you, you have to provide or input the necessary information and complete the registration process by such means or in such manner prescribed by us from time to time.

(c) At any time where the same Proxy ID is registered by you for more than one account (whether maintained with us or with any other Participant), you must set one account as the Default Account. By instructing us to set or change the Default Account for you, you consent and authorise us to submit the request on your behalf to HKICL FPS to override the existing Default Account registered in HKICL FPS.

4. eDDA Service

(a) In order to enable us to handle a request for you in relation to eDDA setup, you have to provide or input the necessary information and complete the process by such means or in such manner prescribed by us from time to time. The prescribed process may include requiring the relevant parties to set up the eDDA using their respective account numbers or customer identification numbers or codes. For the avoidance of doubt, a Proxy ID is not intended for verifying eDDA setup. Any amendment of a Proxy ID and the related records or termination of a Proxy ID after an eDDA setup will not affect that eDDA.

(b) You hereby authorise us to effect transfers from your account to that of the beneficiaries in accordance with such instructions as we may receive from the beneficiaries from time to time provided always that the amount of any one such transfer shall not exceed the limit indicated in the eDDA setup.

(c) You agree that we shall not be obliged to ascertain whether or not notice of any such transfer has been given to you.

(d) You accept full responsibility for any overdraft (or increase in existing overdraft) on your account which may arise as a result of any such transfer(s) conducted in accordance with the eDDA setup.

(e) You agree that should there be insufficient funds in your account to meet any transfer, we shall be entitled, in our discretion, not to effect such transfer in which event we may charge you the usual fees.

(f) The eDDA shall remain in effect until you have provided us at least one(1)-week advanced notification for cancellation or variation of your eDDA setup or until after your designated end date as specified in the eDDA setup (whichever shall first occur).

(g) You agree that any notice of cancellation or variation of the authorisation for a specific direct debit transaction will only become effective once the counter-party confirms the cancellation or variation request.

(h) If the amount of your payments is likely to vary each time, you agree that you will set the limit for each payment at the maximum amount you expect to pay at any one time in the eDDA setup.

5. Your responsibility

(a) Present genuine owner or authorised user of Proxy ID and accounts

You can only register your own Proxy ID for your own accounts or set up eDDA for your own accounts. You must be the present genuine owner or authorised user of each Proxy ID and each account provided to us for registration in the Addressing Service and the eDDA Service. By instructing us to register any Proxy ID or any account for you in relation to the Faster Payment System, you confirm that you are the present genuine owner or authorised user of the relevant Proxy ID or account. This is particularly important for mobile phone numbers as they may be recycled in Hong Kong.

(b) Proxy ID

Any Proxy ID to be registered by you for the Addressing Service must satisfy any applicable requirements imposed by HKICL from time to time. For example, HKICL may require the mobile phone number or email address to be registered as Proxy ID to be the same number or address registered by you as contact information on our records at the relevant time. You understand and agree that we, other Participants and HKICL have the right and discretion without giving notice to deregister any Proxy ID that is not correct or up-to-date in accordance with available information without your consent.

(c) Correct information

(i) You have to ensure that all the information provided by you for registration or amendment of Proxy ID (or any related records) or for any eDDA setup is correct, complete, up-to-date and not misleading. You have to notify us as soon as reasonably practicable of any changes or updates to such information by such means or in such manner specified by us from time to time.

(ii) You are fully responsible for using the correct and up-to-date Proxy ID and related records in giving each payment or funds transfer instruction. You are solely liable for and will hold us harmless from any incorrect payment or transfer effected by us and HKICL FPS due to incorrect or outdated Proxy ID or related records.

(d) Timely updates

(i) You are fully responsible for giving instructions and information changes or updates to us on a timely basis for amending your Proxy ID (or related records) or any eDDA setup, including without limitation changing your Default Account, or terminating any Proxy ID or eDDA. You acknowledge that keeping your Proxy ID, eDDA and all related records up-to-date is critical for ensuring effective execution of payment and funds transfer instructions and for avoiding incorrect payment or transfer due to incorrect or outdated Proxy ID, eDDA or related records.

(ii) You may liable if loss is caused by your failure to provide update information which may result in the Bank being unable to process your applications or to provide or continue to the eDDA Service and/or the related services to you.

(e) Change of Default Account

If an account is terminated as the Default Account by you or by the relevant Participant for any reason (including suspension or termination of the account), the system of HKICL will automatically assign the most recently registered record in the Addressing Service that is associated with the same Proxy ID to be the Default Account. If you wish to set another account as the Default Account, you have to change the registration through the Participant where you maintain that other account.

(f) Transactions binding on you

(i) For any payment or funds transfer, once you confirm the details of a transaction and submit instruction to us, such instruction and any resulting transaction is final, irrevocable and binding on you.

(ii) For any Proxy ID registration or eDDA setup, once you submit an instruction to us, such instruction is irrevocable and binding on you. You may amend or cancel any Proxy ID or eDDA setup in accordance with the procedures and requirements prescribed by us from time to time.

(g) Use Bank Services responsibly

You must use the Bank Services in a responsible manner. In particular, you have to comply with the following obligations:

(i) You must comply with all Regulatory Requirements that govern your use of the Bank Services, including collecting, using and handling the personal data and other information relating to any other person in compliance with the Regulatory Requirements protecting data privacy. You must not use the Bank Services for any unlawful purposes or any purposes other than those authorised or contemplated in the rules, guidelines and procedures of HKICL.

(ii) In sending remarks or messages to be displayed to recipients or counterparties of your payment or funds transfer instructions or eDDA setup using HKICL FPS, you should mask the name or other data of such recipients or counterparties to prevent unauthorised display or disclosure of any personal data or confidential data.

(iii) If we offer the FPS ID as Proxy ID to you, you should not repeatedly cancel the registration and request for generation of another FPS ID in an attempt to generate a number or value that you desire.

(h) Other obligations regarding payments and funds transfers

Any instruction given by you in relation to the Bank Services will be handled by us in accordance with these Terms and Conditions and the applicable provisions in the Existing Terms. You have to comply with the other obligations with respect to payments, funds transfers and direct debit authorisations, including without limitation maintaining sufficient funds in the relevant accounts for settling payment and funds transfer instructions from time to time.

(i) You are responsible for your authorised persons

Where you authorise any other person to give instructions or requests to us in connection with the use of the Bank Services (whether you are an individual, a company, a corporation, or a sole proprietorship or partnership firm or any other unincorporated body):

(i) you are responsible for all the acts and omissions of each person authorised by you;

(ii) any instruction or request received by us, believed by us in good faith to be given by you or any person authorised by you, will be irrevocable and binding on you; and

(iii) you are also responsible for ensuring that each person authorised by you will comply with the provisions of these Terms and Conditions that are applicable to him/her when acting on your behalf.

6. Our responsibility and restriction of liability

(a) We will process and submit your instructions and requests to HKICL FPS in accordance with the applicable rules, guidelines and procedures imposed by HKICL from time to time. HKICL FPS has the right to process and execute your instructions and requests in such sequence or manner as HKICL considers appropriate. We have no control over the operation of HKICL FPS nor the timing on which your instructions or requests are executed by HKICL FPS. Where we receive status update notifications involving any of your Proxy ID (or related records) or eDDA setup or any other matter relating to HKICL FPS from or through HKICL FPS from time to time, we will notify you accordingly by such means and at such time as we consider appropriate.

(b) Without reducing the effect of Clause 6(a) above or the provisions of the Existing Terms:

(i) we are not liable for loss, damage or expense of any kind which you or any other person may incur or suffer arising from or in connection with the use of the Bank Services or the processing or execution of instructions or requests given by you in relation to the Bank Services or HKICL FPS, except to the extent that any loss, damage or expense incurred or suffered is direct and reasonably foreseeable arising directly and solely from our negligence or wilful default or that of our officers, employees or agents;

(ii) for clarity, we are not liable for loss, damage or expense of any kind which you or any other person may incur or suffer arising from or in connection with one or more of the following:

(1) your failure to comply with your obligations relating to the Bank Services; and

(2) any delay, unavailability, disruption, failure, error of or caused by HKICL FPS, or arising from any circumstances beyond our reasonable control; and

(iii) in no event will we, our affiliates or group companies, our licensors, and our and their respective officers, employees and agents be liable to you or any other person for any loss of profit or any special, indirect, incidental, consequential or punitive loss or damages (whether or not they were foreseeable or likely to occur).

(c) Your confirmation and indemnity

(i) Without reducing the effect of any indemnity given by you under the Existing Terms or any other rights or remedies that we may have, you will indemnify us and our officers, employees and agents and hold each of them harmless against all liabilities, claims, demands, losses, damages, costs, charges and expenses of any kind (including legal fees on a full indemnity basis and other expenses reasonably incurred) which may be incurred or suffered by us or any of them and all actions or proceedings which may be brought by or against us or any of them as a result of or in connection with our provision of the Bank Services or your use of the Bank Services.

(ii) The above indemnity does not apply to the extent that it is proved that any liabilities, claims, demands, losses, damages, costs, charges, expenses, actions or proceedings are direct and reasonably foreseeable arising directly and solely from our negligence or wilful default or that of our officers, employees or agents. The above indemnity shall continue to have effect after the termination of the Bank Services.

7. Collection and use of Customer Information

(a) For the purposes of using the Bank Services, you may be required to provide us with the personal data and other information relating to one or more of the following persons from time to time:

(i) yourself;

(ii) the recipient of any payment or funds transfer to be made by you, or the counterparty of any eDDA to be set up by you; and

(iii) where you are a company, a corporation, or a sole proprietorship or partnership firm or any other unincorporated body, any of your directors, officers, employees, authorised persons and representatives,

all personal data and information provided to us or compiled by us from time to time in connection with the Bank Services are collectively referred to as "Customer Information".

(b) You agree (and, where applicable, for and on behalf of each of your directors, officers, employees, authorised persons and representatives) that we may collect, use, process, retain or transfer any of the Customer Information for the purposes of the Bank Services. These purposes include without limitation one or more of the following:

(i) providing the Bank Services to you, maintaining and operating the Bank Services;

(ii) processing and executing your instructions and requests in relation to the Bank Services from time to time;

(iii) disclosing or transferring the Customer Information to HKICL and other Participants for their use for the purpose of the operation of HKICL FPS;

(iv) meeting the requirements to make disclosure under any Regulatory Requirements; and

(v) purposes relating to any of the above.

(c) You understand and agree that the Customer Information may be further disclosed or transferred by HKICL, us or any other Participants to their customers and any other third parties who are users of HKICL FPS for the purposes of providing and operating the Addressing Service and the eDDA Service.

(d) If the Customer Information includes personal data or other information of any person other than yourself (including any persons specified in Clauses 7(a)(ii) or 7(a)(iii) above), you confirm that you will obtain and has obtained the consent from such person regarding the use (including disclosure and transfer) of his/her personal data and other information by HKICL, us and the other Participants as specified in this Clause.

Schedule II Terms and Conditions for i-Token Service and Biometric Authentication

i-Token Service is provided by The Bank of East Asia, Limited (the "Bank") to the Customer on the following Terms and Conditions.

1. Registration

1.1 By registering and/or subscribing for i-Token Service or Biometric Authentication, the Customer and the Customer's Authorised User(s) shall be regarded as having accepted and bound by the provisions of these Terms and Conditions.

1.2 The Customer and the Customer's Authorised User(s) shall be able to register i-Token for the purpose of the System. The Customer shall exercise due care and good internal control within its operations from time to time and to implement segregation of duties with the Customer's Authorised User(s). The Bank shall be under no obligation to investigate or verify the authority of any person effecting the instructions given by any Customer's Authorised User(s) on behalf of the Customer.

2. Definitions and Interpretation

2.1 In these Terms and Conditions, words and expressions below shall have the following meanings:-

"ATM" means:	any automated teller machine of the Bank.
"Administrator" means:	has the same meaning as such term is defined under the Bank's Terms and Conditions for Corporate Cyberbanking and BEA Corporate Online Services (as amended from time to time).
"Authorised Person" means:	has the same meaning as such term is defined under the Bank's Terms and Conditions for Corporate Cyberbanking and BEA Corporate Online Services (as amended from time to time).
"Mobile App" means:	mobile application offered by the Bank through which a Customer Authorised User can access the System and i-Token Service (as amended from time to time).

	“Biometric Authentication” means:		the identity authentication function in Mobile 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 the System, Mobile App or other electronic delivery channels as designated by the Bank from time to time.
	“Customer” means:		any entity, sole proprietorship, partnership or corporation (which shall include its representative and lawful successor) who has applied for i-Token Service and whose representative applies for i-Token Service and/or Biometric Authentication.
	“Customer’s Authorised User” means:		with respect to Corporate Cyberbanking, any Signer(s) authorised by the Customer from time to time. with respect to BEA Corporate Online, any of the user(s) (including but not limited to Authorised Person(s), Signer(s), Administrator(s), Normal User(s)) who is/are authorised by the Customer from time to time.
	“i-Token” means:		a device binding unique identifier which could be downloaded to Mobile App and stored in the key-chain (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.
	“i-Token PIN” means:		the personal identification number designated and used by a Customer’s Authorised User(s) to authenticate the access to the System and other delivery channels as announced by the Bank from time to time, and to confirm transactions performed via the individual electronic delivery channels.
	“i-Token Service” means:		the service provided by the Bank to the Customer and/or Customer’s Authorised User(s) from time to time in relation to i-Token as two-factor authentication method, to enable a Customer’s Authorised User(s) to use i-Token PIN/ Biometric Authentication to login and/or confirm transactions in the System and/or Mobile App via the designated mobile device(s).

"Normal User" means:	has the same meaning as such term is defined under the Bank's Terms and Conditions for Corporate Cyberbanking and BEA Corporate Online Services (as amended from time to time).
"PIN" means:	any personal identification number assigned to a Customer's Authorised User(s) which may be used to access the System, ATM and/or other designated channel(s) as designated by the Bank from time to time and authenticate transactions in such channel(s).
"Notification" means:	a message from the Bank that is sent to a Customer's Authorised User's designated mobile device or such other form(s) of electronic notification as prescribed by the Bank from time to time.
"Signer" means:	has the same meaning as such term is defined under the Bank's Terms and Conditions for Corporate Cyberbanking and BEA Corporate Online Services (as amended from time to time).
"SMS" means:	short message service which is a service for sending short messages to the designated mobile devices.
"System" means:	has the same meaning as such term is defined under the Bank's Terms and Conditions for Corporate Cyberbanking and BEA Corporate Online Services (as amended from time to time).

2.2 These Terms and Conditions is a schedule to and supplement and form part of the Bank's Terms and Conditions for Corporate Cyberbanking and BEA Corporate Online Services (as amended from time to time). Unless otherwise specified, the provisions of these Terms and Conditions prevail if there is any inconsistency between them and the other provisions of the Bank's Terms and Conditions for Corporate Cyberbanking and BEA Corporate Online Services (as amended from time to time) insofar as the inconsistency relates the i-Token Service, Biometric Authentication and/or Mobile App.

2.3 If any of these Terms and Conditions become invalid or unenforceable at any time, the validity and/or enforceability of any of the other terms and conditions hereof shall not be affected.

2.4 Where the context permits, the singular includes the plural and vice versa, the masculine includes feminine and neuter and vice versa.

3. **i-Token Service**

3.1 i-Token provides an alternative means of verifying a person's identity for accessing the System and other delivery channels as announced by the Bank from time to time. Each of the

Administrators of Corporate Cyberbanking and each of the Customer's Authorised User(s) of BEA Corporate Online 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, relevant Customer's Authorised User shall use his/her password associated with i-Token Service (instead of the user name and password for Mobile App, the System or the relevant delivery channels) to confirm his/her identity for accessing the System.

3.2 If there is any change to the designated mobile device for i-Token Service, the registrant should follow the installation and activation procedures of i-Token as prescribed by the Bank from time to time.

3.3 Updates to i-Token may be required periodically. The registrant may not be able to use i-Token if the latest version of Mobile App has not been downloaded to the designated mobile device(s) for i-Token Service.

3.4 The Customer agrees and understands that Notification by the Bank shall be received through the inbox of Mobile App of the relevant Customer's Authorised User or alternatively, an SMS will be sent directly to the designated mobile device(s) of the relevant Customer's Authorised User by the Bank for notification purpose before the relevant Customer's Authorised User signs and executes the transactions. The Bank shall only notify the relevant Customer's Authorised User(s) in respect of any transactions pending for signing via Notification or SMS. The Customer's Authorised User(s) shall check the inbox of Mobile App and the designated mobile device(s) regularly from time to time and contact the Bank if such Notification or SMS is not received.

3.5 Notification or SMS shall be deemed to be received by the relevant Customer's Authorised User(s) immediately after transmission.

3.6 Any instructions or transactions given, approved, confirmed or executed by a Customer's Authorised User(s) via i-Token Service is/are not allowed to 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 given, approved, confirmed or executed by the relevant Customer's Authorised User(s). 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 given, approved or executed by the Customer or any Customer's Authorised User(s) via i-Token Service as the Bank thinks appropriate.

3.8 The Bank shall only be required to retain the record of incomplete or pending for approval instructions on or before the relevant execution date (or such other date as prescribed by the Bank from time to time) (the "Due Date") and the Customer/Customer's Authorised User(s) shall approve or execute the transactions on or before the Due Date. Upon receiving Notification or SMS from the Bank through the designated mobile device(s), the relevant Customer's Authorised User(s)

shall examine each Notification or SMS on a timely basis and take follow-up action accordingly. Those incomplete instructions would become invalid if such transactions have not been approved or executed by the relevant Customer's Authorised User(s) via i-Token Service after the Due Date.

4. Biometric Authentication (applicable to BEA Corporate Online)

4.1 Biometric Authentication provides an alternative means of verifying a Customer's Authorised User's identity for accessing the System. A Customer's Authorised User(s) may register such of his/her mobile device as may be specified by the Bank from time to time (with biometric sensor supported) for Biometric Authentication by completing the steps specified by the Bank.

4.2 By undergoing the enabling process to use Biometric Authentication, or using Biometric Authentication, the Customer's Authorised User accepts and agrees that Biometric Authentication 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 Authorised User's mobile device which has been successfully registered for Biometric Authentication, and the Customer's Authorised User hereby consents to the Bank accessing and using such information for identity authentication of the Customer's Authorised User before provision of Biometric Authentication.

4.3 Once the Customer's Authorised User has successfully enabled Biometric Authentication in his/her mobile device, the Customer's Authorised User may use his/her biometric credentials registered with his/her mobile device in lieu of his/her User ID/the Customer's account number/Username and mobile password/Personal Identification Number ("PIN"), or i-Token PIN to authenticate his/her identity to access and operate the Customer's account(s) maintained with the Bank, and/or confirm transactions in the System or other electronic delivery channels as announced by the Bank from time to time.

4.4 The Customer's Authorised User must not use facial recognition for Biometric Authentication if the Customer's Authorised User (i) has identical siblings, or (ii) is an adolescence where his/her facial features may be developing rapidly. The Customer's Authorised User must not compromise or disable the security settings of his/her biometric credentials registered in the Customer's Authorised User'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 Authorised User's sole and exclusive use.

4.5 Biometric Authentication is under Mobile App and may only be available for mobile devices supporting biometric authentication as prescribed by the Bank from time to time. Biometric Authentication may not work if the mobile device contains applications not compatible with Biometric Authentication.

4.6 To use Biometric Authentication, the Customer's Authorised User shall ensure that Mobile App has been installed on his/her mobile device and be a valid user of the System.

4.7 To enable Biometric Authentication, the Customer's Authorised User must go through an enabling process that verifies any one type of his/her biometric credentials registered on the mobile device, and the Customer's Authorised User is required to key in his/her credentials of channel(s), as specified by the Bank from time to time for authentication.

4.8 Each time the designated software detecting the use of the biometric credential(s) registered on the Customer's Authorised User's mobile device on which the Customer's Authorised User has enabled Biometric Authentication to access and operate the Customer's account, the Customer's Authorised User is deemed to have (i) accessed and/or (ii) operated the Customer's account in lieu of his/her User ID/the Customer's account number/Username and mobile password/PIN, or i-Token, and/or (iii) instructed the Bank to perform such transactions (as the case may be).

4.9 If the Customer's Authorised User believes that the security of his/her biometric credential(s) has been compromised, the Customer's Authorised User must cease and/or re-enable the use of the System and change the relevant passwords, and notify the Bank immediately. The Bank may require the Customer's Authorised User to change the relevant passwords and/or biometric credential(s) registered in his/her mobile device, to cease and/or re-enable the use of Mobile App, the System and/or Biometric Authentication.

4.10 The Customer's Authorised User confirms that all information provided to the Bank at the time of registration to use Biometric Authentication is true, complete and up-to-date. The Customer's Authorised User must also ensure that all information provided to the Bank from time to time remains true, complete and up-to-date and notify the Bank of any change in the information as soon as reasonably practicable. The Customer's Authorised User 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 Biometric Authentication (or any part thereof); and (b) gain access to Biometric Authentication (or any part thereof) in any manner other than specified by the Bank.

4.11 The authentication is performed by the Mobile App by interfacing with the biometric identity sensor module on the Customer's Authorised User's mobile device. The Bank does not collect the biometric credentials of the Customer's Authorised User. The Mobile App will access the biometric identity sensor in the Customer's Authorised User's mobile device and obtain the necessary information to perform the authentication. The Customer's Authorised User consents to the authentication process and the Bank's access and use of the information obtained through the biometric identity sensor.

5. Mobile Devices

5.1 Each of the Customer's Authorised User(s) must comply with all applicable laws and regulations governing the installation, download and access of i-Token/Mobile App. The Customer or the relevant Customer's Authorised User(s) shall be the genuine owner of the designated mobile device(s) and must not use or allow any other person to use i-Token/Mobile App for any unauthorised purpose. The Bank shall not be liable for any losses or any other consequences suffered or incurred by the Customer and the Customer's Authorised User(s) as a result thereof.

5.2 Each of the Customer's Authorised User(s) undertakes to take all reasonable precautions to keep safe and prevent fraudulent use of the 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 and the Customer's Authorised User(s) liable for all unauthorised transactions and all direct and indirect losses or damages arising therefrom. The Bank may in its sole discretion update the security precautionary measures in relation to i-Token/Mobile App and the Customer and the Customer's Authorised User(s) shall at all times follow such security precautionary measures accordingly.

5.3 The Customer and the Customer's Authorised User(s) must not access or use i-Token/Mobile App 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 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 manufacturer without their approval. Access or use of i-Token/Mobile App on a jail broken or rooted device may compromise security and lead to fraudulent transactions. Use of i-Token/Mobile App in a jail broken or rooted device is entirely at the own risk of the Customer and each of the Customer's Authorised User(s). The Bank shall not be liable for any losses or any other consequences suffered or incurred by the Customer or the Customer's Authorised User(s) as a result thereof.

6. Liabilities and Indemnity

6.1 The liabilities and obligations of the Customer and the Customer's Authorised User(s) under these Terms and Conditions shall be joint and several. All transactions effected by the Bank through use of i-Token, Biometric, Mobile App or the System shall be binding on the Customer and the Customer's Authorised User(s) in all respects. The Customer shall procure and ensure that each of the Customer's Authorised User(s) shall fully comply with these Terms and Conditions and shall be responsible for all the acts, omissions and negligence of or on the part of each of the Customer's Authorised User(s).

6.2 The Customer and the Customer's Authorised User(s) accept that i-Token Service, Biometric Authentication, Mobile App and the System 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/Mobile App by the Bank due to strikes, power failures, change in law, rules or regulations or other calamity.

6.3 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 6.2 above or any breach or failure to perform the Bank's obligations due to abnormal and unforeseeable circumstances or any other causes beyond the Bank's reasonable control or anticipation. Under no circumstances shall the Bank be liable to the Customer and the Customer's Authorised User(s) 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, Mobile App or the System. The Bank's liability (if any) to the Customer and the Customer's Authorised User(s) for loss in relation to the provision of i-Token Service, Biometric Authentication, Mobile App or the System shall only be limited to the amount of the relevant transaction or the direct and reasonably foreseeable damages sustained whichever is less.

6.4 i-Token Service, Biometric Authentication, Mobile App and the System 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). The Bank shall not be responsible for any loss suffered by the Customer and the Customer's Authorised User(s) or any third party as a result of the access or use of i-Token Service, Biometric Authentication, Mobile App or the System by the Customer or the Customer's Authorised User(s).

6.5 The Bank shall not assume any responsibility or obligation for any transaction or error due to the failure of the Customer or any of the Customer's Authorised User(s) to provide or input sufficient or accurate data which result in the relevant transaction failing to be materialized or effected through i-Token Service, Biometric Authentication, Mobile App or the System.

6.6 The Customer and each of the Customer's Authorised User(s) shall indemnify and keep the Bank indemnified against any consequences, claims, proceedings, losses, damages or expenses (including all legal costs on a full indemnity basis) (save and except for those loss or damages caused by negligence or wilful default or fraud on the part of the Bank) incurred or sustained by the Bank arising from or in connection with (i) the provision by the Bank of i-Token Service and Biometric Authentication; or (ii) breach of any of these Terms and Conditions by the Customer and the Customer's Authorised User(s).

6.7 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 and Biometric Authentication or in relation to the processing of or any other request relating to i-Token Service and Biometric Authentication. Without prejudice to the foregoing, the Customer and the Customer's Authorised User understand and acknowledge the acceptance by the Bank of their respective submission of a request through use of i-Token Service or Biometric Authentication does not amount to a representation or warranty by the Bank:

(a) i-Token Service or Biometric Authentication will meet requirements of the Customer and the Customer's Authorised User(s);

(b) i-Token Service or Biometric Authentication 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 i-Token Service or Biometric Authentication or the Bank's processing of any request will be uninterrupted timely, secure or free of any virus or error.

6.8 Save and except due to the negligence or wilful default of the Bank, the Bank shall not be liable and the Customer and the Customer's Authorised User(s) agree to indemnify the Bank and keep

the Bank indemnified against any consequences, claims, proceedings, losses, damages or expenses (including all legal costs on any indemnity basis) whatsoever and howsoever caused that may arise or be incurred by the Bank in providing i-Token Service and Biometric Authentication, whether or not arising from or in connection with and including but not limited to the following:

(a) any improper or unauthorised use of i-Token Service or Biometric Authentication or the relevant software by the Customer or the Customer's Authorised User(s);

(b) any act or omission by any relevant mobile or internet service provider;

(c) any delay or failure in any transmission, dispatch or communication facilities;

(d) any access (or inability or delay in accessing) and/or use of i-Token Service or Biometric Authentication or the relevant software; or

(e) any breach of warranty under or provision of these Terms and Conditions.

6.9 The Bank shall be entitled to exercise any of its rights and remedies under these Terms and Conditions (including the right to withdraw, restrict, suspend, vary or modify i-Token Service, Biometric Authentication, Mobile App, the System and/or other software (whether in whole or in part)).

7. Suspension and Termination

7.1 The Bank has the absolute discretion at any time as it deems fit to modify, cancel, suspend or terminate i-Token Service without giving reasons and without prior notice to the Customer or the Customer's Authorised User(s). If i-Token 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 or the Customer's Authorised User(s) in connection with such cancellation, suspension or unavailability.

7.2 Without prejudice to Clauses 7.1 and 7.5, the Customer and the Customer's Authorised User(s) acknowledge that the Bank shall be entitled to terminate i-Token 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/Mobile App or any elements thereof;

(b) the Customer and the Customer's Authorised User commit any breach of or omits to observe any obligations under these Terms and Conditions which, in the sole opinion of the Bank, amounts to a breach or default on the part of the Customer and the Customer's Authorised User.

7.3 Each of the Customer and the Customer's Authorised User(s) shall acquire appropriate mobile device(s) with requisite specifications and system requirement which enables i-Token/Mobile App to be installed therein and undertake to ensure that such mobile device(s) shall not cause any

damage to i-Token/Mobile App whether by virus, other contaminating or destructive properties or by any reasons whatsoever. Each of the Customer and the Customer's Authorised User(s) shall also procure installation of the updates and the latest version of i-Token/Mobile App in the designated mobile device(s) from time to time.

7.4 The Customer and each of the Customer's Authorised User(s) agree and acknowledge that installation and registration for i-Token or Biometric Authentication is free-of-charge but the Bank reserves the right to levy fees and charges against the Customer and the Customer's Authorised User(s) to cover the running and operating costs for i-Token or Biometric Authentication in the future. Each of the Customer and the Customer's Authorised User(s) shall be solely responsible for any fees or charges that the telecommunication carrier may charge in connection with the transmission of data or the use of i-Token or Biometric Authentication.

7.5 When a Customer's Authorised User leaves employment with the Customer or is no longer authorised to use i-Token or Biometric Authentication, the Customer shall disable Mobile App, i-Token and Biometric Authentication for that Customer Authorised User accordingly. The Bank shall not be responsible for any loss suffered by the Customer if such Customer Authorised User continues to access or use Mobile App, i-Token or Biometric Authentication without permission.

7.6 If the Customer or any of the Customer's Authorised User becomes aware of any loss, theft or unauthorised use of the designated mobile device(s) or reasonably believe or suspect that any other person knows the Customer's security details, the Customer and the Customer's Authorised User undertakes to report such incident to the Bank immediately and the Customer and the Customer's Authorised User shall disable the relevant i-Token immediately. In such circumstances, the Bank is entitled to deny any subsequent access to or activation of i-Token by the Customer and the Customer's Authorised User(s) and terminate i-Token Service accordingly.

7.7 The Customer and the Customer's Authorised User(s) acknowledge 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, Biometric Authentication or Mobile App. The Bank may use such information, as long as it is in a form that does not personally identify the Customer or the Customer's Authorised User(s) to improve its products or to provide services or technologies.

Schedule III Terms and Conditions for Open Application Programming Interface Service and Third Party Service Provider Consent Management Service

In consideration of The Bank of East Asia, Limited ("BEA" or the "Bank") agreeing to provide the Open Application Programming Interface Service ("Open API Service") and the Third Party Service Provider Consent Management Service ("Consent Management Service", together with "Open API Service", are collectively referred to as the "API Services") through the Bank's Open API Webpage, BEA Corporate Online, Mobile App (for BEA Corporate Online) or other electronic delivery channels as announced by BEA from time to time, I/we (the "Customer") understand and hereby agree that by using any of the API Services, the following terms and conditions (as amended from

time to time by the Bank) ("these Terms and Conditions"), together with the Terms and Conditions for Corporate Cyberbanking and BEA Corporate Online Services and The Personal Data (Privacy) Ordinance – Personal Information Collection (Customers) Statement of the Bank ("PICS"), shall be binding on the Customer. In the event of any conflict between these Terms and Conditions and the Terms and Conditions for Corporate Cyberbanking and BEA Corporate Online Services, these Terms and Conditions shall apply and prevail insofar as the API Services are concerned.

1. Open Application Programming Interface Service

(a) Open API Service allows third party service providers ("**TSP**") to access the Customer's account information, such as account availability, account status, account balance and transaction details. By using the Open API Service, the Customer can check his/her own bank account information through the website or mobile applications of or provided by the TSP.

(b) The Bank will not share with or transfer to TSP the account information of the Customer without his or her consent given in accordance with these Terms and Conditions.

(c) By proceeding further to use the Consent Management Service after being redirected from the TSP, the Customer will need to access the TSP website or mobile app and the Customer shall be deemed to have read and accepted the terms and conditions governing the TSP's platform and agreed to be bound by them.

2. Third Party Service Provider Consent Management Service

(a) In order to use the Consent Management Service, the Customer must be an Authorised Person of BEA Corporate Online and shall at all times follow the authentication procedures of the API Services as prescribed by the Bank from time to time.

~~(a)~~(b) The Customer may apply the API Services to all or any designated account(s) linked with any one of the Related Accounts and Associated Accounts (as respectively defined in the Terms and Conditions for Corporate Cyberbanking and BEA Corporate Online Services) of BEA Corporate Online account.

~~(b)~~3. Grant Consent

The purpose of the consent under this Clause 3 is to enable the Customer to give permission to the Bank to transfer the account information as specified to the TSP using the Bank's Open API service for the purpose(s) that the Customer has consented to and subscribed with the TSP who has directed the Customer to the Bank's Open API service.

The Customer may log into the TSP website or Mobile App and select the Bank to initiate the grant consent request. Upon selection, the TSP may display the consent details including the purpose for which the data are to be accessed, types of data to be accessed and consent expiry date. The Customer shall review the consent details and select to grant consent to the TSP. The Customer may then be redirected from the TSP's website or mobile app to the Bank's Open API Webpage.

The Customer has to log into BEA Corporate Online through the Bank's Open API Webpage by completing the authentication procedure of the Consent Management Service as prescribed by the Bank from time to time.

The Customer may select all or designated a list of the available accounts with consent details. The Customer should review the details of consent information including but not limited to the TSP name, consent expiry date, renewal of consent and select the account(s) for which consent will be granted. The Customer should also read, confirm and acknowledge these Terms and Conditions for Open Application Programming Interface Service and Third Party Service Provider Consent Management Service and The Personal Data (Privacy) Ordinance – Personal Information Collection (Customers) Statement of the Bank before confirming to grant the consent.

The customer will be logged out from BEA Online Banking from the Bank's Open API Webpage and redirected to the TSP's website or mobile app in order to complete the grant consent action. Upon completion, the Bank will notify the Customer the grant consent details through SMS, email or the notification channel as prescribed by the Bank from time to time.

4. Renew Consent

The Customer has to pay attention to the renewal notification from TSP and act accordingly. Otherwise, the TSP will not be able to access the Customer's account information when the consent expires. Also, the Bank bears no liability for any loss or damage arising out of or resulting from the suspension of the TSP services.

The Customer may log into the TSP website or mobile app and the TSP may notify the Customer for renewal of consent on or before the expiry date. The TSP may display the designated bank account consent details including the purpose for which the data are to be accessed, types of data to be accessed and consent expiry date. The Customer should review the consent details and select for renewal of consent to the TSP. The Customer may then be redirected from the TSP's website or mobile app to the Bank's Open API Webpage.

The Customer has to log into BEA Corporate Online through the Bank's Open API Webpage by completing the authentication procedure of the Consent Management Service as prescribed by the Bank from time to time.

In the event that the consent is renewed, the Customer will be logged out from BEA Corporate Online from the Bank's Open API Webpage and redirected to the TSP's website or mobile app in order to complete the renewal process. Upon completion, the Bank will notify the Customer the renewed consent details through SMS, email or notification channel as prescribed by the Bank from time to time.

5. Revoke Consent

(a) Through TSP website or mobile app

The Customer may log into the TSP website or mobile app or the channels provided/prescribed by the TSP to revoke the consent and select the Bank to initiate the revoke consent request. Upon selection, the TSP may display the consent details including the purpose for which the data are to

be accessed, types of data to be accessed and consent expiry date. The Customer should first review the consent details before confirming the revocation of the consent to the TSP.

(b) Through BEA Corporate Online or Mobile App (for BEA Corporate Online)

The Customer may log into the BEA Corporate Online or Mobile App (for BEA Corporate Online) to initiate the consent revocation request. Upon selection, the Bank will display the consent details including the purpose for which the of data are to be accessed, types of data to be accessed and consent expiry date. The Customer should first review the consent details before confirming the revocation of the consent to the TSP.

In the event that the consent is revoked through either of the above channels, the Bank will notify the Customer of the revocation through the email or notification channel as prescribed by the Bank from time to time.

The customer data to which the consent relates will not be shared with the TSP after the relevant consent has been revoked by the Customer through the above channels or in condition that the Cyberbanking account or its linked account has been closed by the Customer and the collaboration or business relationship with TSP has been terminated. The Customer should contact the TSP directly to understand the implications of revoking the consent including the handling of historical customer data, data retention period, data retention purpose and the handling process when data is no longer required. The Bank bears no liability of any loss arising out of or resulting from the suspension of the service by TSPs.

6. Liabilities and Indemnity

6.1. The Customer accepts that the API Services 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 Customer's equipment, devices or facilities 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 the API Services by the Bank due to strikes, power failures, change in law, rules or regulations or other calamity.

6.2. The Bank and its subsidiaries, affiliates, agents, officers and employees shall not be liable for the occurrence of any of the events as described in Clause 6.1 above or any breach or failure to perform the Bank's obligations due to abnormal and unforeseeable circumstances 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 the API Services. The Bank's liability (if any) to the Customer for loss in relation to the provision of the API Services shall only be limited to the reasonably foreseeable damages sustained by the Customer.

6.3. The API Services are provided upon Customer's request on "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 Customer's equipment, devices or facilities. 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 the API Services by the Customer.

6.4. The Bank shall not assume any responsibility or obligation for any error due to the failure of the Customer to provide or input sufficient or accurate data and his/her failure to update the mobile phone number(s), email address or other information which result in the relevant transaction failing to be materialized or effected through the API Service.

6.5. 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 the API Services or in relation to the processing of or any other request relating to the API Services. Without prejudice to the foregoing, the Customer understands and acknowledges the acceptance by the Bank of his/her submission of a request through use of the API Services does not amount to a representation or warranty by the Bank:

(a) The API Services will meet the Customer's requirements;
(b) The API Services 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 API Services or the Bank's processing of any request will be uninterrupted timely, secure or free of any virus or error.

6.6. Save and except due to the negligence or wilful default of the Bank, the Bank shall not be liable and the Customer agrees to indemnify the Bank and keep the Bank indemnified against any consequences, claims, proceedings, losses, damages or expenses (including all legal costs on any indemnity basis) whatsoever and howsoever caused that may arise or be incurred by the Bank in providing the API Services, whether or not arising from or in connection with and including but not limited to the following:

(a) any improper or unauthorized use of the API Services;
(b) any act or omission by any relevant internet service provider;
(c) any delay or failure in any transmission, dispatch or communication facilities;
(d) any access (or inability or delay in accessing) and/or use of the API Services or the relevant software; or
(e) any breach of warranty under any provision of these Terms and Conditions.

6.7. The Bank shall be entitled to exercise any of its rights and remedies under these Terms and Conditions (including the right to withdraw, restrict, suspend, vary or modify the API Services and/or other software (whether in whole or in part)).

6.8. The Bank Under no circumstances shall the Bank be liable to the Customer for the marketing materials post on the TSP's website or mobile app. The products and services provided by TSP are not owned, controlled or affiliated with the Bank. The Customer will bear all the risks of using the TSP's website or mobile app. The Bank is not responsible for the contents therein and/or the Customer's use of them.

7. Suspension and Termination

7.1. The Bank has the absolute discretion at any time as it deems fit to modify, cancel, suspend or terminate the API Services without giving any reason and without prior notice to the Customer. If the API Services are 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.

7.2. Without prejudice to Clauses 7.1, the Customer acknowledges that the Bank shall be entitled to terminate the API Services 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 the API Services or any elements thereof;

(b) the Customer commits any breach of or omits to observe any obligations under these Terms which, in the sole opinion of the Bank, amounts to a breach or default on the part of the Customer.

7.3. The Customer agrees and acknowledges that, registration and uses for the API Services is 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 the API Services in the future. The Customer shall be solely responsible for any fees or charges that may be incurred in connection with the use of the API Services (including but not limited to any charges imposed by the TSP).