TERMS AND CONDITIONS FOR I-TOKEN SERVICE AND BIOMETRIC AUTHENTICATION FOR BEA APP

This document sets out the terms and conditions for i-Token Service and Biometric Authentication for BEA App (as amended, modified and/or supplemented from time to time) (the "**Terms**") provided by the Bank of East Asia, Limited, Singapore Branch ("**BEA**" or the "**Bank**"). These Terms shall be subject to and read in conjunction with the Terms and Conditions for SG Cyberbanking Service (Corporate Banking) or the Terms and Conditions for SG Cyberbanking Service (Personal Banking), as may be applicable (the "**Cyberbanking Terms**").

1. Registration

1.1 By registering and/or subscribing for i-Token Service or Biometric Authentication, the Customer shall be regarded as having accepted and agreed to be bound by the provisions of these Terms.

2. Definitions and Interpretation

Capitalised terms used but not defined in these Terms shall have the meaning given to them (if any) in the relevant Cyberbanking Terms. In these Terms, unless the context otherwise requires, the following expressions shall have the following meanings:

2.1 "**BEA App**" means the software made available by the Bank and designates to run on smartphones and other mobile devices to provide the services as specified by the Bank from time to time;

2.2 "**Biometric Authentication**" means the identity authentication function in BEA App through which biometric credentials, including but not limited to fingerprint, facial map and/or any other biometric credentials, can be accessed and used to confirm transactions in Cyberbanking, BEA App or other electronic delivery channels as designated by the Bank from time to time;

2.3 "**Customer**" in the context of Corporate Cyberbanking Service includes the Customer's User(s) where applicable;

2.4 "**Inbox Message**" means a message from the Bank that is sent to the Customer's designated mobile device or such other form(s) of electronic notification as prescribed by the Bank from time to time;

2.5 "**i-Token**" means a device binding unique identifier which could be downloaded to BEA App of the Customer and stored in the keychain (or other security area described by the Bank from time to time) of the designated mobile device after successful registration of i-Token Service with the Bank;

2.6 "**i-Token Service**" means the service provided by the Bank to the Customer from time to time in relation to i-Token as two-factor authentication method, to enable the Customer to use i-Token PIN/ Biometric Authentication to login and/or confirm transactions in Cyberbanking Service and/or BEA App via the designated mobile device(s);

2.7 "**Security Code**" means an one-time numerical code generated through i-Token Service to login and/or confirm transactions via electronic delivery channels;

2.8 "**SMS**" means short message service which is a service for sending short messages to the designated mobile devices;

2.9 "**i-Token PIN**" means the personal identification number designated and used by the Customer to authenticate the access to BEA Mobile Banking, Cyberbanking Services and other delivery channels as announced by the Bank from time to time, and to confirm transactions performed via the individual electronic delivery channels.

2.10 These Terms are additional to, and not in substitution for, any other applicable terms and conditions governing the services provided by the Bank to the Customer. If any of these Terms becomes invalid or unenforceable at any time, the validity and/or enforceability of any of the other terms and conditions hereof shall not be affected. In the event of any conflict or inconsistency between any of the provisions of these Terms and the provisions of the relevant Cyberbanking Terms, the provisions of the relevant Cyberbanking Terms shall prevail to the extent of the conflict or inconsistency.

3. i-Token Service

3.1 i-Token provides an alternative means of verifying the Customer's identity for accessing Cyberbanking Service and other delivery channels as announced by the Bank from time to time. The Customer may register for i-Token Service on such mobile devices as may be specified by the Bank from time to time by completing the steps specified by the Bank. Once successfully registered, the Customer shall use the password associated with i-Token Service (instead of the Customer name and password for BEA App, BEA Mobile Banking, Cyberbanking or the relevant delivery channels) to confirm his identity for accessing Cyberbanking Service, to the extent such i-Token access is made available by the Bank.

3.2 If there is any change to the Customer's designated mobile device for the i-Token Service, the Customer should follow the procedures for installing and activating the i-Token on the Customer's new mobile device, as prescribed by the Bank from time to time.

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

3.4 The Customer agrees and understands that the Bank will send an Inbox Message to the BEA App for redirecting to login to different electronic delivery channels or to confirm transactions using i-Token PIN or Biometric Authentication. The Bank shall only notify the Customer in respect of any transactions pending for confirmation via Inbox Message. The Customer shall check for Inbox Messages on the BEA App regularly from time to time and contact the Bank if any expected notifications are not received.

3.5 Inbox Messages shall be deemed to be received by the Customer immediately after transmission.

3.6 Any instructions or transactions confirmed or executed by the Customer via the Customer's registered credentials on the i-Token Service may not be rescinded or withdrawn. All such instructions or transactions, when confirmed and acknowledged by the Bank in accordance with the relevant approval process applicable to the Customer, shall be irrevocable and binding on the Customer regardless of whether or not such instructions or transactions are confirmed or executed by the Customer or its Authorised Person, or by any other person purporting to be the Customer or its Authorised Person. The Bank shall be under no duty to verify the identity

or authority of the person giving any such instructions or signing such transactions or the authenticity of such instructions or transactions which shall be conclusive and binding on the Customer in any event.

3.7 The Bank may at all times and from time to time in its sole discretion without having to state the grounds for such refusal and without any liability whatsoever, refuse to act upon any instructions or transactions confirmed or executed by the Customer via i-Token as the Bank thinks appropriate.

3.8 Upon receiving any Inbox Message or Push Notification from the Bank through BEA App, the Customer shall examine the Inbox Message or Push Notification on a timely basis and take follow-up action accordingly. Any Instruction or transaction may be considered in the Bank's discretion to be incomplete or invalid if the relevant Instruction or transaction is not confirmed by the Customer via i-Token by the stipulated time.

3.9 The i-Token Service is provided by the Bank subject to such restrictions as may be notified by the Bank from time to time. In particular, not all types of accounts are eligible to use the i-Token Service.

3.10 If the Customer believes that the security of their i-Token has been compromised, the Customer must cease the use of Cyberbanking Service, change the relevant passwords, and notify the Bank immediately. The Bank may require the Customer to change the relevant passwords and/or the i-Token registered in their mobile device, to cease and/or re-enable the use of BEA Mobile Banking, Cyberbanking Service and/or i-Token Service.

4. Biometric Authentication

4.1 Biometric Authentication provides an alternative means of verifying the Customer's identity for accessing the Cyberbanking Service. The Customer may register their mobile device (with biometric sensor supported) that meets the technical for Biometric Authentication by completing the registration steps specified by the Bank.

4.2 By registering to use Biometric Authentication or using Biometric Authentication, the Customer accepts and agrees that the Biometric Authentication Service will access the biometric credentials (including but not limited to fingerprint, facial map and/or any other biometric credentials as prescribed by the Bank from time to time) recorded and stored in the Customer's mobile device which has been successfully registered for Biometric Authentication, and the Customer hereby consents to the Bank accessing and using such information for the purposes of Biometric Authentication, including to authenticate the identity of the Customer.

4.3 Once the Customer has successfully enabled and registered for Biometric Authentication in their mobile device, the Customer may use their biometric credentials registered with Biometric Authentication to confirm their identity for accessing the Cyberbanking Service, to the extent such Biometric Authentication access is made available by the Bank.

4.4 The Customer must not use facial recognition for Biometric Authentication if the Customer (i) has identical siblings, or (ii) is an adolescent where their facial features may be developing rapidly. The Customer must not compromise or disable the security settings of their biometric credentials registered in the Customer's mobile device, including but not limited to disabling passcode to access the biometric credentials, and/or disabling "attention aware" features for facial recognition. Biometric Authentication is provided for the Customer's personal use only.

4.5 To use Biometric Authentication, the Customer shall ensure that the BEA App has been installed on their mobile device and be a valid Customer of BEA Mobile Banking. The Customer

acknowledges that the availability of Biometric Authentication is subject to the compatibility and technical specifications of their mobile device.

4.6 Any instructions or transactions confirmed or executed by the Customer via Biometric Authentication may not be rescinded or withdrawn. All such instructions or transactions, when confirmed and acknowledged by the Bank in accordance with the relevant approval process applicable to the Customer, shall be irrevocable and binding on the Customer regardless of whether or not such instructions or transactions are confirmed or executed by the Customer or its Authorised Person, or by any other person purporting to be the Customer or its Authorised Person. The Bank shall be under no duty to verify the identity or authority of the person giving any such instructions or signing such transactions or the authenticity of such instructions or transactions which shall be conclusive and binding on the Customer in any event.

4.7 If the Customer believes that the security of their biometric credential(s) has been compromised, the Customer must cease the use of the Cyberbanking Service, change the relevant passwords, and notify the Bank immediately. The Bank may require the Customer to change the relevant passwords and/or biometric credential(s) registered in their mobile device, to cease and/or re-enable the use of Cyberbanking Service and/or Biometric Authentication.

5. Mobile Device(s)

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

5.2 The Customer undertakes to take all reasonable precautions to keep safe and prevent fraudulent use of their designated mobile device(s) and its security information. Non-compliance of security precautionary measures as prescribed by the Bank from time to time would render the Customer liable for all 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, Biometric Authentication, BEA App, BEA Mobile Banking and/or Cyberbanking Service and the Customer shall at all times follow such security precautionary measures accordingly.

5.3 The Customer must not access or use i-Token Service, Biometric Authentication, BEA App or Cyberbanking Service through any device or operating system that has been modified outside the mobile device or operating system vendor supported or warranted configurations. This includes but is not limited to devices that have been "jail-broken" or "rooted". A jail broken or rooted device means one that has been freed from the limitations imposed on it by the designated mobile service provider and the phone or device manufacturer without their approval. Access or use of i-Token Service, Biometric Authentication, BEA App or Cyberbanking on a jail broken or rooted device may compromise security and lead to fraudulent transactions. Use of i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking and/or Cyberbanking Service in a jail broken or rooted device is entirely at the own risk of the Customer. The Bank shall not be liable for any losses or any other consequences suffered or incurred by the Customer as a result thereof.

5.4 The Customer shall acquire appropriate mobile device(s) with requisite specifications and system requirement which enables i-Token Service, Biometric Authentication, BEA Mobile

Banking and/or BEA App to be installed and used therein and undertake to ensure that such mobile device(s) shall not cause any damage to i-Token Service, Biometric Authentication, BEA Mobile Banking and/or BEA App whether by virus, other contaminating or destructive properties or by any reasons whatsoever. The Customer shall also procure installation of the updates and the latest version of i-Token, Biometric Authentication and BEA App in the designated mobile device(s) from time to time.

5.5 The Customer agrees and acknowledges that installation and registration for i-Token Service and/or Biometric Authentication are generally free-of-charge but the Bank reserves the right to levy fees and charges against the Customer to cover the running and operating costs for i-Token Service and Biometric Authentication in the future. The Customer shall be solely responsible for any fees or charges that their telecommunication carrier may charge in connection with the transmission of data or the use of i-Token Service and Biometric Authentication.

5.6 The Customer 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 Service, Biometric Authentication, BEA Mobile Banking and/or BEA App. The Bank may use such information, as long as it is in a form that does not personally identify the relevant Customer to improve its products or to provide services or technologies.

5.7 The Customer understands the need to protect their mobile device, including but not limited to set a passcode of their mobile device and not permit any other persons to register their biometric credentials in their mobile device and/or use i-Token Service or Biometric Authentication.

6. Liabilities and Indemnity

6.1 The liabilities and obligations of the persons comprising the Customer under these Terms shall be joint and several. All transactions effected by the Bank through use of i-Token, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Services shall be binding on the Customer in all respects.

6.2 The Customer accepts that i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking and Cyberbanking may be subject to various information technology risks or force majeure events beyond the Bank's control, including but not limited to:

a. inaccuracy, interruption, interception, mutilation, disruption, unavailability, delay or failure relating to data transmission, communication network or internet connection;
b. unauthorised access by other persons (including hackers);
c. damage to the designated mobile device(s) caused by virus, other contaminating or destructive properties or by any reasons whatsoever;
d. malfunction, breakdown or inadequacy of equipment, installation or facilities; or
e. failure to provide i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking 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, fraud or negligence by the Customer, or any other causes beyond the Bank's reasonable control or anticipation. Under no circumstances shall the Bank be liable to the Customer or Customer for any incidental, indirect or consequential or exemplary damages including, without limitation,

any loss of use, revenue, profits or savings (whether foreseeable by the Bank or not) arising out of or related to the access or use of i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service. The Bank's maximum liability (if any) to the Customer for loss in relation to the provision of i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Service shall 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, BEA App, BEA Mobile Banking and Cyberbanking Services 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 or any third party as a result of the access or use of i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking Services by the Customer.

6.5 The Bank shall not assume any responsibility or obligation for any transaction or error due to the failure of the Customer to provide or input sufficient or accurate data which result in the relevant transaction failing to be materialized or effected through i-Token Service, Biometric Authentication, BEA App or Cyberbanking Services.

6.6 The Customer 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 willful 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 by the Customer.

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 understands and acknowledges the acceptance by the Bank of his/her 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 the Customer's requirements;
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 fault 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 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;
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.

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

7. Suspension and Termination

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

7.2 Without prejudice to Clause 7.1, the Customer acknowledges that the Bank shall be entitled to terminate i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking immediately upon occurrence of any of the following events:

a. there is any change of law which prohibits or renders illegal the maintenance or operation of i-Token Service, Biometric Authentication, BEA App, BEA Mobile Banking or Cyberbanking or any elements thereof;
b. the Customer commits any breach of or omits to observe any obligations under these Terms.

7.3 If the Customer becomes aware of any loss, misuse of Biometric Authentication, theft or unauthorised use of the designated mobile device(s) or reasonably believe or suspect that any other person knows the Customer's Security Details, the Customer undertake to report such incident to the Bank immediately and shall disable i-Token and Biometric Authentication on their mobile device(s) immediately. In such circumstances, the Bank is entitled to deny any subsequent access to BEA App, BEA Mobile Banking or Cyberbanking Service, or activation of i-Token, use of Biometric Authentication by the Customer and terminate the i-Token Service or Biometric Authentication for the Customer accordingly.

7.4 The Customer can terminate i-Token Service or Biometric Authentication registered in his/her mobile device in BEA App or such other channel as accepted by the Bank at any time. Any termination of i-Token Service or Biometric Authentication shall not affect the Customer's liabilities and obligations which have incurred or accrued and any instruction provided to the Bank prior to such termination. The Bank may suspend or terminate i-Token Service or Biometric Authentication at any time without giving any notice or reason.

8. Amendments

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

9. Contracts (Rights of Third Parties) Act

9.1 A person who is not a party to these Terms shall have no right under the Contracts (Rights of Third Parties) Act (Chapter 53B) to enforce any of its terms.

10. Governing Law and Jurisdiction

10.1 These Terms are governed by and construed in accordance with the laws of Singapore. The courts of Singapore shall have exclusive jurisdiction to settle any dispute which may arise out of or in relation to the Terms, and the parties submit to such jurisdiction.

11. Governing Version

11.1 These Terms are only available in English. Words and phrases in the Terms shall be read and construed in accordance with the definitions contained hereto. Where the context permits, the singular includes the plural and vice versa, the masculine includes feminine and vice versa.