BEA東亞銀行

BEA Online Terms and Conditions for i-Token Service and Biometric Authentication

i-Token Service and Biometric Authentication are provided by The Bank of East Asia, Limited ("BEA" or "the Bank") to the Customer on the following terms and conditions:

1. Registration

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 and Conditions.

2. Definitions and Interpretation

2.1 In these Terms and Conditions, unless the context otherwise requires, the following expressions shall have the following meanings:-

"BEA Mobile" (also known as "BEA App") means:	the software made available by the Bank and designates to run on smartphones and other mobile devices as BEA may designate from time to time to provide the banking services offered by the Bank in accordance with the BEA Online Terms and Conditions;
"BEA Online" (also known as "Cyberbanking") means:	various electronic banking services including BEA Mobile (also known as "BEA App", collectively called "BEA Online") offered by the Bank in accordance with the BEA Online Terms and Conditions over different electronic delivery channels as prescribed by the Bank from time to time, including but not limited to the internet, mobile devices, fixed line telephone networks and Automatic Teller Machines;
"Biometric Authentication" means:	the identity authentication function in BEA Mobile 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 BEA Online or other electronic delivery channels as designated by the Bank from time to time;
"Customer" means:	any individual who (i) is the holder of an account opened and maintained with the Bank; and (ii) applies for i-Token Service or i-Token Service with Biometric Authentication;
"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;
"i-Token" means:	a device binding unique identifier which could be downloaded to BEA Mobile 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;
"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 BEA Online and/or BEA Mobile via the designated mobile device(s);
"QR Code" means:	the QR Code provided by the Bank for the Customer to scan and capture the transaction data without the need for manually entering the data;
"Security Code" means:	an one-time numerical code generated through i-Token Service to login and/or confirm transactions via electronic delivery channels;

"SMS" means:	short message service which is a service for sending short messages to the designated mobile devices;
"i-Token PIN" means:	the personal identification number designated and used by the Customer to authenticate the access to BEA Mobile, BEA Online and other delivery channels as announced by the Bank from time to time, and to confirm transactions performed via the individual electronic delivery channels.

2.2 These Terms and Conditions 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 and Conditions 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.

2.3 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 the Customer's identity for accessing BEA Mobile, BEA Online 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 user name and password for BEA Mobile, BEA Online or the relevant delivery channels) to confirm his identity for accessing BEA Mobile or BEA Online.

3.2 If there is any change to the designated mobile device for i-Token Service, the Customer 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 Customer may not be able to use i-Token if the latest version of BEA Mobile has not been downloaded to the designated mobile device(s) for i-Token Service.

3.4 The Customer agrees and understands that the Bank will send Inbox Message to BEA Mobile or alternatively, the Customer will scan QR Code displayed at BEA Online with the Customer's designated mobile device(s), for redirecting to login to different electronic delivery channels or 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 the Inbox Message of BEA Mobile regularly from time to time and contact the Bank if such notification is not received.

3.5 Inbox Message 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 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 confirmed or executed by the Customer or by any other person purporting to be the Customer. The Bank shall be under no duty to verify the identity or authority of the person giving any such instructions or signing such transactions or the authenticity of such instructions or transactions which shall be conclusive and binding on the Customer in any event.

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

3.8 Upon receiving any Inbox Message or push notification from the Bank through BEA Mobile, the Customer shall examine the Inbox Message or push notification on a timely basis and take follow-up action accordingly. The incomplete instruction would become invalid if the relevant transaction is not confirmed by the Customer via i-Token after the due time.

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

4. Biometric Authentication

4.1 Biometric Authentication provides an alternative means of verifying the Customer's identity for accessing BEA Mobile and BEA Online. The Customer may register such of his 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 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 mobile device which has been successfully registered for Biometric Authentication, and the Customer hereby consents to the Bank accessing and using such information for identity authentication of the Customer before provision of Biometric Authentication.

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

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

4.5 Biometric Authentication is under BEA Mobile 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 shall ensure that BEA Mobile has been installed on his/her mobile device.

4.7 To enable Biometric Authentication, the Customer must go through an enabling process that verifies any one type of his/her biometric credentials registered on the mobile device, and the Customer is required to key in his/her credentials of channel(s), as specified by BEA 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 mobile device on which the Customer has enabled Biometric Authentication to access and operated his/her account, the Customer is deemed to have (i) accessed and/or (ii) operated his/her account in lieu of his/her User ID/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 believes that the security of his/her biometric credential(s) has been compromised, the Customer must cease and/or re-enable the use of BEA Mobile and BEA Online and 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 his/her mobile device, to cease and/or re-enable the use of BEA Mobile, BEA Online and Biometric Authentication.

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

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 Mobile and/or BEA Online. The Customer shall be the sole owner of the designated mobile device(s) and must not use or allow any other person to use the i-Token, Biometric Authentication, BEA Mobile and/or BEA Online 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 and Conditions.

5.2 The Customer 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 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 Mobile and/or BEA Online 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 Mobile or BEA Online 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 Mobile or BEA Online on a jail broken or rooted device may compromise security and lead to fraudulent transactions. Use of i-Token Service, Biometric Authentication, BEA Mobile and/or BEA Online 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 and/or BEA Mobile 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 and/or BEA Mobile 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 Mobile 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 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 the 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 acknowledges that the Bank may collect, store and use technical data and related information, including but not limited to information about the designated mobile device(s), system and application software, peripherals and other personal information that is gathered periodically to facilitate the provision of software updates, product support and other services (if any) related to i-Token Service, Biometric Authentication and/or BEA Mobile. The Bank may use such information, as long as it is in a form that does not personally identify the Customer to improve its products or to provide services or technologies.

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

5.8 Each mobile device may only bind one i-Token.

6. Liabilities and Indemnity

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

6.2 The Customer accepts that i-Token Service, Biometric Authentication, BEA Mobile and BEA Online 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 Mobile or BEA Online 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 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 Mobile or BEA Online. The Bank's maximum liability (if any) to the Customer for loss in relation to the provision of i-Token Service, Biometric Authentication, BEA Mobile or BEA Online 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 Mobile and BEA Online 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 Mobile or BEA Online 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 Mobile or BEA Online.

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 and Conditions 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 unauthorized 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 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, BEA Online, BEA Mobile 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, Biometric Authentication, BEA Mobile or BEA Online without giving reasons and without prior notice to the Customer. If i-Token Service, Biometric Authentication, BEA Mobile or BEA Online 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 Mobile or BEA Online 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 Mobile or BEA Online or any elements thereof;

(b) the Customer commits 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 material breach or default on the part of the Customer.

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 undertakes to report such incident to the Bank immediately and shall disable i-Token and Biometric Authentication immediately. In such circumstances, the Bank is entitled to deny any subsequent access to BEA Mobile or BEA Online, 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 via the "Settings" page in BEA Mobile 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

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 binding on the Customer if the i-Token Service or Biometric Authentication is continued to be used after the effective date thereof, and such revisions shall be deemed to be accepted.

9. Contracts (Rights of Third Parties) Ordinance

No party other than the Bank and the Customer shall have any right under the Contracts (Rights of Third Parties) Ordinance (Cap. 623 of the laws of Hong Kong) to enforce or enjoy the benefit of any of the provisions of these Terms and Conditions.

10. Governing Law and Jurisdiction

These Terms and Conditions are governed by and construed in accordance with the laws of the Hong Kong Special Administrative Region of the People's Republic of China and the courts of such place shall have non-exclusive jurisdiction to settle any dispute which may arise out of or in relation to these Terms and Conditions.

11. Governing Version

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.