中国建设银行(亞洲)
China Construction Bank (Asia)

China Construction Bank (Asia) Corporation Limited – Customer Awareness Terms and Conditions in relation to Open Application Programming Interface (Open API) (For Enterprises)

1. Application, Definitions, and Interpretation

1.1. Application

1.1.1. The Bank strives to provide seamless customer experience and deliver innovative banking products and services to its customers through its collaboration with TSPs and the use of the Bank API.

1.1.2. The Bank API facilitates the Bank to share or exchange its product information or banking information about its customers with TSPs using an open application programming interface. Customers may benefit from the following services:

(a) the Customer would be able to view the latest information and promotional offers of the Bank's products and services (and those of other banks) on a TSP Application. Customers may compare different banking services and products under a single website or mobile application and apply for these banking products and services via the TSP Application;

(b) upon receiving the Customer's authorisation, the Bank may share bank account information of the Customer (e.g., account availability, status, balance and transaction details) with a TSP. The Customer would be able to use the TSP Application to view its bank account information held with multiple banks; and

(c) the Customer may perform online fund transfers and payments to third parties through the TSP Application.

1.1.3. These Terms apply where the Customer elects to: (a) grant its consent to allow the Bank to share the Open Data with a TSP; (b) renew the consent to enable the TSP to continue accessing the Open Data from the Bank; (c) revoke the consent if it no longer wants the TSP to use and access the Open Data; and (d) participate in any other applicable TSP collaboration.

1.1.4. These Terms also set out important information about the Bank's collaboration with a TSP, which the Customer should read carefully.

1.1.5. These Terms are supplemental to, and should be read together with, the Terms and Conditions for Accounts and Related Services (For Enterprise Customers) (the "**Master TC**").

1.1.6. These Terms may be amended at any time, or the Bank may introduce additional terms and conditions to these Terms from time to time. The amended Terms will become effective upon the Bank giving reasonable notice to the Customer, including posting the amended Terms on the Mobile Banking App, on the Website or displaying the amended Terms in the Bank’s branches (where appropriate).

1.1.7. If there is any inconsistency between the provisions in these Terms, the Master TC and such other terms and conditions, these Terms will prevail insofar as the sharing of Open Data with a TSP and the Bank's collaboration with a TSP is concerned.

1.1.8. The Bank may at any time and for whatever reason, suspend or terminate the sharing of the Open Data with the TSP and the Bank API without prior notice to you or the TSP. You agree that the Bank shall not be liable for any loss arising out of or in connection with such suspension or termination.

1.2. Definitions and Interpretation

1.2.1. In these Terms, unless otherwise specified, all defined terms in the Master TC shall have the same meaning when used in these Terms.

1.2.2. In these Terms:

"**Bank APIs**" means the application programming interface(s) made available by the Bank to the TSP from time to time to enable the TSP's access to the Open Data;

"**Open Data**" means the data about the Customer (such as the Customer's bank account information) that is made available by the Bank to the TSP through the Bank APIs from time to time;

"**TSP**" means a third-party service provider, including among others other banks and financial services providers, that provides certain products and/or services to the Customer by accessing and making use of the Open Data or other data provided to it by the Bank; and

"**TSP Application**" means the user interface of the TSP, whether in the form of a website or mobile application, which the TSP uses to provide its products and services to its customers (including the Customer).

2. Customer Consent Management

2.1. A Customer can grant, renew and revoke consent (either from the TSP Application or the Online Enterprise Banking Services as the case may be) to the TSP's or the Bank’s access to the Open Data in the manner described below. For details, the Customer should refer to the steps and procedures specified in the relevant TSP Application and the Online Enterprise Banking Services, where applicable.

2.1.1. **Granting Consent:** Through the platform operated by data consumer (whether through the TSP Application or the Online Enterprise Banking Services (as appropriate)), the Customer initiates the grant consent request, reviews the relevant consent details and is redirected to the platform operated by the data provider for authentication of the Customer's identity. After the Customer completes the authentication and the granting of consent processes, it will be redirected back to the platform operated by the data consumer (whether TSP Application, the Bank API or Online Enterprise Banking Services (as appropriate)) and presented with a successful grant consent confirmation page.

2.1.2. **Renewing Consent:** Through the platform operated by the data consumer (whether through the TSP Application or the Online Enterprise Banking Services (as appropriate)), the Customer receives a notification to renew its consent to allow the continued access to the Open Data by the data consumer. The Customer proceeds to review the relevant consent details and elects to renew consent. The Customer is then redirected to the platform operated by the data provider for authentication of the Customer's identity. After the Customer completes the authentication, it will be redirected to the the platform operated by the data consumer (whether the TSP Application or the Online Enterprise Banking Services (as appropriate)) and presented with a successful renew consent confirmation page.

2.1.3. **Revoking Consent through the TSP Application:**

(a) The Customer accesses the consent management dashboard on the TSP Application and selects the bank account (i.e., an account opened and maintained with the Bank) to initiate a revoke consent request.

(b) Upon selection, the Customer reviews the consent details and elects to revoke consent to the TSP's access to the Open Data.

(c) The TSP Application informs the Customer of the implications of such consent revocation, which the Customer would review and accept such implications.

(d) The Customer confirms the consent revocation request and is presented with a successful revoke consent confirmation page.

2.1.4. **Revoking Consent through the Online Enterprise Banking Services:**

(a) The Customer accesses the consent management dashboard through the Online Enterprise Banking Services and selects the bank account to initiate a revoke consent request.

(b) Upon selection, the Customer reviews the consent details and elects to revoke consent to the TSP's access to the Open Data.

(c) The Customer confirms the consent revocation request and is presented with a successful revoke consent confirmation page.

(d) Alternatively, the Customer's consent will be deemed to be revoked upon the occurrence of the following events: (i) the Bank terminates the Customer's use of the Online Enterprise Banking Services; or (ii) closure of all of the Customer's accounts held with the Bank.

2.2. The Bank is entitled to rely on and treat all consents originated from the TSP Application as being properly obtained, and to be final and conclusive. With such consent, the Bank is authorized and is deemed to be authorized by the Customer to share the Open Data to the TSP.

2.3. The Bank shall not be liable for any loss arising from error, omission, delay, interruption or process in the Customer’s granting, renewing and revoking of the Customer’s consent.

3. The Open Data

3.1. The Bank will only use the Bank API to share and access personal details or bank account information of the Customer upon obtaining the Customer's consent. The Bank will not share the Customer's banking credentials including the User Names, Passwords, Security Codes, etc. with a TSP under any circumstances.

3.2. When the Customer authorises the Bank to share the Open Data with the TSP, the TSP will only use such data to provide certain products and services to the Customer through the TSP Application. For details of the types of Open Data that will be used by the TSP (and for what purpose) and the specific product or service provided by the TSP, the Customer shall refer to the relevant TSP Application.

3.3. When the TSP is the data consumer, the Customer understands that the TSP will:

3.3.1. be able to read but not amend the Customer's bank account information held with the Bank;

3.3.2. with the Customer's consent, make or process fund transfers or payments to third parties on the Customer's behalf;

3.3.3. not have access to the Customer's login credentials to the Online Enterprise Banking Services, including the User Names, Passwords, Security Codes, etc.;

3.3.4. not be able use or access any Open Data without the Customer's consent; and/or

3.3.5. not use any Open Data for marketing purposes unless the Customer has granted its consent or has not objected to such use.

3.4. The Customer agrees that it may modify or revoke its consent to the Bank’s and the TSP's access to the Open Data at any time via the means described in Clause 2.1.3 and 2.1.4 above. For details on how the Customer can revoke its consent, it should refer to the specific steps and procedures described in the Online Enterprise Banking Services and the TSP Application.

3.5. The Customer acknowledges that any Open Data held by the TSP or the Bank, to the extent that it is "personal data" (as defined in the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong)), is held in line with the requirements under the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong).

4. Using the Open API safely

4.1. Before engaging a TSP, the Customer should confirm that the identity and website address of the products and/or services provided by the TSP and the name of the TSP Application are listed on the Bank's TSP Partners' list as amended and updated by the Bank from time to time.

4.2. The Bank shall not be liable for any TSP that is not listed on the TSP Partners' list, as well as any TSP products and/or services outside of the TSP's collaboration with the Bank.

4.3. When using the TSP Application, the TSP may collect the Customer's personal data for their own use. When considering whether to provide personal data to the TSP, the Customer understands that the TSP may or may not have the same privacy standards and data storage standards as the Bank's. The Customer shall ensure that it has read the TSP's service agreement and privacy policy and will pay attention to the information requested and the permissions granted to such TSP to use the Customer's information.

4.4. The Customer shall carry out its own risk-assessments, make its own enquiries and verify the information provided by the TSP on the TSP Application independently.

4.5. Generally, disclosing to or allowing any third party to acquire or use banking credentials belonging to the Customer, such as the User Names, Passwords, Security Codes and other account information, could expose the Customer to various risks, including unauthorized transactions and personal data leakage. The Customer should understand the scope of the permission it is granting to a third party and these associated risks, before disclosing any banking credentials to third parties. The Bank will not be liable or responsible for any losses that the Customer may suffer or incur in relation to the above.

4.6. The Customer acknowledges and accepts that the TSP collaborating with the Bank is not owned, controlled or affiliated with the Bank. The Customer shall bear any risks of using the TSP Application. The Bank is not responsible or liable for the contents therein and/or the Customer's use of the TSP Application or reliance of any contents therein or any contents shared by the TSP (if any). Furthermore, by collaborating with the TSP, the Bank shall not be deemed to endorse, recommend, approve, guarantee, offer, solicit or introduce TSP's products and/or services (whether on the TSP Application or otherwise).

4.7. To protect the Customer's information and interest, the Customer must not provide any of its information to any suspected caller or call any suspected hotline number. If the Customer is in doubt about the identity of the caller or hotline number, the Customer should request for the callers' contact details and call the Bank's 24-Hour Bogus Calls Enquiry hotline at 3179 5504 for verification.

4.8. Should the Customer have any queries or complaints concerning the TSP's products and/or services, the TSP Application, any information requested by any TSP (including those listed on the Bank's TSP Partners' list as amended and updated by the Bank from time to time), the contents shared by the TSP (if any) and/or the Bank's collaboration with the TSP, it should promptly direct any such queries or complaints to the Bank's customer service service hotline at 2903-8366 or email at CorporateEBankingSupport@asia.ccb.com .

4.9. To keep the Open Data secure, the Customer agrees to adopt: (a) the security safeguards in the Master TC when accessing the Online Enterprise Banking Services; and (b) the following security safeguards when accessing the TSP Application:

4.9.1. keep mobile telephones and other electronic devices ("**Devices**") used to access the TSP Application under the Customer's personal control at all times, and not to share such Devices with anyone else;

4.9.2. keep any account credentials, passwords, security codes, biometric credentials (such as the Customer's fingerprint, facial map or any other biometric data) and other security details (together, the "**Security Details**") used to access the TSP Application secure and confidential;

4.9.3. refrain from setting Security Details (particularly passwords) that are easy to guess (e.g., refrain from including information such as the Customer's birthday, telephone number or a recognizable part of his or her name) and using the same Security Details to access other services or mobile applications on his or her Device;

4.9.4. take reasonable precautions to prevent loss, theft or unauthorised or fraudulent use of his or her Devices, Security Detail and/or other confidential information;

4.9.5. only use the Customer's own Device to access the TSP Application and if the Customer uses someone else's Device, to ensure it is secure and that the Customer has completely logged-off the abovementioned services;

4.9.6. refrain from using the TSP Application on any Device or operating system of such Device that has been modified outside the Device or the operating system vendor's supported or warranted configurations. This includes Devices that have been "jail-broken" or "rooted". The use of the TSP Application on a "jail broken" or "rooted" Device may compromise security and lead to fraudulent transactions;

4.9.7. install the appropriate anti-virus, personal firewall software and other security software to protect the Device that the Customer uses to access the TSP Application, from computer viruses, Trojan horses, worm viruses or other malware;

4.9.8. safeguard against social engineering techniques used to obtain the Customer's information such as the Security Details through fake or suspicious emails, websites or mobile applications or impersonation of the Bank's staff or the police, and to report any of the above irregularities to the Bank immediately;

4.9.9. promptly check any advice, statements or notifications received from the Bank, and to notify the Bank as soon as practicable by contacting the Bank's staff through the designated means, whenever unauthorised or unusual transactions or observations are detected;

4.9.10. adopt proper dual controls and authorization before conducting any high-risk transactions through the TSP Application;

4.9.11. only use the TSP Application downloaded from approved or designated mobile application stores (such as those operated by Apple or Google); and

4.9.12. where applicable, only access the TSP Application by typing the authentic website address into the browser or by bookmarking the genuine website for subsequent access and not to access any of the above websites or applications through hyperlinks embedded in emails, internet search engines or suspicious pop-up windows.

5. Bank API

5.1. The Bank will use reasonable skill and care to ensure that the Bank API are secure and do not contain viruses or other damaging property, however, the Bank cannot guarantee that this will be the case or that no damage will occur to the Open Data, software, computer, mobile device or other digital content. The Bank accepts no liability for any failure of the Bank API due to circumstances beyond its control or any act or omission of any third party.

5.2. The Bank is not responsible for any equipment, software or user documentation which someone other than the Bank produces or any service that the Customer uses which the Bank does not control.

5.3. The Bank will take reasonable care to ensure that any information displayed in the Bank API is accurate. Where information is provided by a third party, the Bank cannot guarantee that it is accurate or error-free.

6. Language

These Terms are drafted in the English language. If any translation of these Terms is made, the English version prevails to the extent of any inconsistency between the English and the Chinese versions.

7. Governing law

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