Cathay United Bank, Singapore Branch
Terms & Conditions Governing
Global MyB2B Service

Terms & Conditions governing "Global MyB2B Service"

1. Scope

(1) These terms and conditions apply to the internet banking service made available by the Bank to the Customer and known as "Global MyB2B Service" ("**Service**"), and shall be read together with the Standard Terms & Conditions Governing Accounts (as amended, varied or supplemented form time to time ("**Standard Terms & Conditions**") which applies to all accounts opened or maintained with the Bank or any banking facilities, products or services provided by the Bank.

(2) In the event of any conflict between these terms and conditions ("**these Terms**") and any other agreement (including the Standard Terms & Conditions), these Terms shall prevail unless the Bank in its sole and absolute discretion otherwise thinks fit.

2. Definitions

In these Terms, unless a contrary indication appears, terms used in the Standard Terms & Conditions (as defined herein) have the same meaning and construction, and:

(1) "Browser" means Internet user interface.

(2) "Certificate" means an electronic attestation signed by the certification authority with a digital signature to verify the identity and qualification of the signatory.

(3) "Corporate Account ID" means the unique identification number assigned to the Customer by the Bank and which forms part of the Customer's login ID for Global MyB2B Service.

(4) "Digital Signature" means an electronic signature generated by the use of mathematic algorithm or other means to create a certain length of digital data from an Electronic Message or Communication encrypted by the signatory's private key, and capable of being verified by the public key.

(5) "Digital Signature Password" (PIN) means an exclusive password for digital signature mechanism to store or activate private key.

(6) "Electronic Message or Communication" means a record carrying text, sound, picture, image, symbol, or other forms of information generated electronically or other means not directly recognizable by human perceptions and transmitted for electronic processing by the Bank or the Customer via computer and network connection that is sufficient to convey the intents of the Bank or the Customer.

(7) "Internet" means an open network using TCP / IP as a communication protocol.

(8) "Global MyB2B Service" means the internet banking service from time to time provided by the Bank, which enables the Customer to access all kinds of banking, network and/or other services provided by the Bank and/or its affiliates from time to time (by giving instructions to, contracting with and/or obtaining information from the Bank and/or its affiliates) through the Internet and/or the Bank's dedicated network(s) at such website(s) or portal(s) as designated by the Bank from time to time, and using computers, mobile devices or through such other means as the Bank may from time to time prescribe;

(9) "PIN" means any personal identification number, code, words, alphabets or password assigned to or selected by any user for access to the Service, or designated for use with any Security Device provided by the Bank.

(10) "Private Key" means certain digital data having parity matching relation and possessed by a signatory to generate a digital signature.

(11) "Public Key" means certain digital data having parity matching relation, made public and used to verify the authenticity of a digital signature.

(12) “Security Device” means any device issued by the Bank to the Customer for the purpose of generating a unique passcode or OTP or PIN to access the Service.

(13) "SSL" (Secure Socket Layer) means a secure encryption mechanism jointly provided by browser at client side and web server at host side to securely protect every record transmitted through network by user.

(14) "User Code" and "User Password" means the pair of username and password which the Customer must provide for verification by the user recognition program of the system in order to access the Global MyB2B service system (whether via the Bank’s dedicated network or the Internet).

3. Access to and Use of Service

(1) By submitting its application form or by its use of the Service, the Customer accepts and agrees to be bound by these Terms and to comply with all guidance from the Bank on the terms of use and any security procedures as may be prescribed by the Bank from time to time for the Service.

(2) The Bank may (but is not obliged to) provide the Service for the Customer, upon the Customer:

i. opening and maintaining at least one account with the Bank;

ii. submitting a completed application form and complying with all relevant identification procedures as the Bank may prescribe from time to time;

iii. providing all relevant corporate approvals, identification documents and any other documents as required by the Bank;

iv. obtaining such security information and implementing such security precautions as required by the Bank.

(3) The Bank is entitled to treat all access and use of the Service as having been duly authorised by the Customer and the records of such use as conclusive evidence of the relevant instruction or communication, unless and until the Bank receives notice of a breach of security or wrongful disclosure of any security information, and the Bank has had a reasonable opportunity to take action in respect of such notice. Without prejudice to the foregoing, the Customer will be liable for any unauthorised transactions arising from or in connection with use of the Service if:

i. the loss is due to fraud, any fraudulent act or gross negligence on the Customer’s part;

ii. the transaction occurred before receipt of notification by the Bank of any security breach and before the Bank has a reasonable opportunity to take action in respect of such notice;

iii. the loss was due to the Customer’s breach of security procedures (including wrongful disclosure of security information or loss/transfer of any Security Device); or

iv. there was delay in the Customer notifying the Bank of any breach of security measures.

(4) The Customer will not be liable for any unauthorised transactions arising from or in connection with use of the Service if the unauthorised transaction is due to the fraudulent or negligent conduct by the Bank’s employees or affiliates involved in the provision of the Service.

(5) The Customer shall comply with all third party terms and conditions (where applicable) in relation to the use of the Service.

4. Authenticity of Website and Network for Connection

(1) The Customer should always confirm and verify the accuracy and authenticity of the website address before proceeding to access or to use the Service, and call the Bank's customer service if the Customer has any enquiries. The Bank shall be under no duty or obligation whatsoever save that the Bank shall use reasonable commercial endeavours in exercising its due diligence as a good manager in constantly maintaining the accuracy and security of its website, and in monitoring for any falsification of its webpages.

(2) The Customer agrees to use the Bank's dedicated network or related network designated by both parties for transmitting Electronic Messages or Communications. For the avoidance of doubt, when using related network designated by both parties, each of the Bank and the Customer shall bear all fees and charges incurred in relation to the access and use of such network (including fees of internet service providers and telecommunication service providers).

5. Risk of Internet Banking Application Environment

(1) The Customer understands that online transactions are not without risks, having regard to the nature of the Internet.

(2) Without prejudice to the foregoing, the Customer shall ensure that its representatives will:

i. pay attention to related software and hardware equipment while using online transaction service;

ii. avoid executing transactions on network equipment provided by Internet café or other unsafe sites;

iii. not disclose any security information (including User Code and User Password) or transfer any Security Device to any third party;

iv. undertake reasonable security precautions to safeguard the security information and Security Device.

(3) The Customer acknowledges and agrees that:

i. the Bank cannot guarantee the complete security of the Customer's instructions and transactions from hacking, unauthorised access, virus attacks and other deliberate attempts by third parties in breaching the security features which have been put in place for the Service (even if the Bank may inform the Customer from time to time of the risks associated with the use of online banking services);

ii. access to and use of the Services are also subject to risks from factors beyond the Bank's control (for example failure of communication networks, mechanical failures, power failures, malfunction, breakdown or inadequacy of equipment and any time lag in communications over the Internet), which may result in the Customer's instructions being delayed, lost or inaccurately transmitted and may cause the Customer to suffer losses.

6. Services

The Customer agrees that all accounts or such accounts maintained by the Customer (as notified by the Customer from time to time in such manner as prescribed by the Bank) may be linked to **Global MyB2B**, in which case account inquiry services and/or payment transfer services will be made available for the Customer's use.

7. Service Hours

(1) Access to and use of the Service for various transactions (including account inquiry and/or payment transfer) shall be conducted and recorded or booked within such service hours as the Bank may implement and in

accordance with relevant regulations of the Bank from time to time.

(2) The Customer acknowledges and agrees that the Bank may from time to time provide for and announce a change in service hours due to the exigencies of the Service.

8. Connection Preparation

(1) The Customer and the Bank agree to use only such designated network(s) for sending and receiving Electronic Messages or Communications in relation to access and use of the Service.

(2) Unless otherwise agreed, the Bank shall only indicate on its website the minimum software and hardware requirements to access and use the Service, and the Customer shall be solely responsible for installing its own computer software and hardware and other security-related equipment required for using the Service. The Customer shall bear all expenses and risks relating to or arising from the installation. If the Customer needs to install additional software and hardware to interface with software and hardware provided by the Bank (whether at the same location or otherwise), such installation must comply with related information provided by the Bank, with the Customer assuming and bearing all related installation expenses and associated risks.

(3) The Customer must have completed all necessary tests before connection if it is so mutually agreed with the Bank.

9. Responsibility for Custody

(1) Access to and use of the Service is on the basis that the Customer shall be solely responsible for all uses of relevant security information, compliance with security precautions, and for all transactions effected. In this regard, the Customer can access the Service only after providing the relevant security information (including the relevant Corporate Account ID, User Code, User Password, OTP or PIN) required by the Bank from time to time.

(2) The Customer shall be responsible for the safe custody of all security information (including the relevant User Code, User Password, OTP or PIN) and for ensuring that all Security Devices (including any software, hardware and related documentation for use of the Service) remain in the possession of its representatives and authorised users at all times.

(3) The Customer acknowledges and agrees to comply with all security measures implemented and instructions issued by the Bank from time to time in relation to the use of the Service, including:

i. the requirement to immediately change User Code and User Password at the first login within such period specified by the Bank to activate the Service;

ii. the automatic restriction against using the Service if any user from the Customer has entered any wrong security information (including User Code, User Password, OTP and PIN, etc) for such number of attempts and/or within such period as specified by the Bank from time to time;

iii. the requirement for the Customer to immediately inform the Bank of any issue with access to or use of the Service;

iv. the requirement for the Customer to apply to lift any automatic restriction or for a new OTP or PIN in order to resume its access to and use of the Service;

v. the requirement to comply with all laws and regulations that may apply to the use of the Service or any banking services made available over the Service;

vi. the requirement to install and update anti-virus, anti-spyware and firewall products with security patches or newer versions of such security products on a regular basis;

vii. the requirement to make regular backups of critical data and to consider the use of encryption technology to protect highly sensitive data.

(4) If the Bank has furnished any software and hardware (including any manual for the use of such software and hardware) for the Customer's use (whether in relation to Clause 8 or otherwise), the Customer may use such software, hardware and relevant documentation only for the purposes of accessing or using the Service. The Customer may not assign, lend or deliver them in any manner to a third party. The Bank retain all rights to such software, hardware and related documentation and shall be entitled (but not obliged) to require the Customer to return such software, hardware and related documentation upon the Customer ceasing to use the Service or the termination of the Service for any reason whatsoever. For the avoidance of doubt, any Security Device provided by the Bank to the Customer remains the property of the Bank and the Customer shall return such Security Device(s) to the Bank promptly upon the Bank's request, upon the Customer ceasing to use the Service, or upon the termination of the Service for any reason whatsoever. Each Security Device must not be altered, tampered with, disassembled or in any way copied, modified or exploited by the Customer in any way.

(5) The Bank may send any security information or Security Device to the Customer by any mode of delivery (including the use of personal delivery or post) to such addresses, email addresses, fax numbers and/or telephone numbers as stated in the Customer's application form or as notified by the Customer from time to time. The Customer agrees to accept all risks associated with the mode of delivery of any security information or any Security Device, and shall not hold the Bank liable in the event that any third party should obtain possession of any security information or Security Device, or if any security information or Security Device fails to reach the Customer.

(6) The Customer must notify the Bank immediately if the Customer reasonably believes that there has been any breach of security (including the wrongful disclosure of any security information, the loss of any Security Device, or the unauthorised transfer / replication of any Security Device). In this regard, the Bank is not deemed to have received any notice unless the Bank has given an acknowledgment in writing. Once the Bank has been notified by the Customer, the Bank will use its reasonable commercial endeavours to revoke the validity of any relevant security information or any Security Device, and to stop the processing of outstanding instructions originating from or related to the breach of security, the relevant security information or the relevant Security Device. Notwithstanding the foregoing, the Customer shall remain responsible for all instructions and transactions which were made prior to the revocation of any security information or Security Device.

10. Authentication and Prevention

(1) The Customer agrees that the users of the Service are divided into authorisation administrators and general users.

(2) The Customer can apply for single control authentication or dual control authentication based on its requirements.

(3) Authorisation administrators can set and manage permissions, accessible items and accounts of general users.

(4) Authorisation administrators and general users can apply for multiple control authentication based on its

requirements. The permissions are divided into makers and supervisors. In order to strengthen monitoring and fraud prevention mechanism, both makers and supervisors login with Corporate Account ID, User Code and User Password. Makers are responsible for data file creation, while supervisors are responsible for review, confirmation, and transmission of the data.

11. Certificate Application, Extension Fees, Scope, and Other Terms of Global MyB2B

(1) The Customer authorises the Bank to deduct applicable fees from designated account when accepting certificate application and extension. The Bank shall announce any change in the applicable fees, the scope of certificate, Global MyB2B URL and related services on the Bank's website.

(2) The Customer can use digital signature to add new business relationships, amend business agreements, modify personal information, and perform transactions on Global MyB2B. The Customer should thoroughly read all kinds of messages (such as directions for certificate application) provided by the Bank, Certificate Organisation, and the Bank's website during application process and agree to comply with agreements in the messages and on Global MyB2B website.

12. One Time Password (OTP)

(1) Instructions

The Customer clearly understands that each set of OTP is generated using random numbers and with characteristics of non-repeatable, used-for-once, and instantaneity. A set of OTP will be invalid if unused within a specified period of time and each set can only be used once. Please refer to the Bank's notification from time to time in relation to the use of OTP.

(2) Wrong Entry and Resumption of Usage

If the Customer enters the wrong OTP for 4 consecutive times or more (as the Bank may specify from time to time), the Bank has the right to terminate or impose a moratorium on the Customer's access to and use of the Service. The Customer must re-apply to lift the moratorium before resuming usage.

(3) Restrictions on Usage

i. The Customer is not allowed to replicate or modify the Security Devices. Performing reverse engineering, decoding, decompiling on software installed on the Customer's registered mobile device under authentication by the Bank, evasion of technology protection measures or replicating the software onto other device are also not allowed.

ii. The Customer shall keep and use its own Security Device. If the Customer lends out, transfers, or pledges its own Security Device, it has sole responsibility for all loss and damage arising.

iii. The Customer shall keep and manage its own Security Device. If the Security Device is lost, destroyed or stolen (regardless of the specific situation), the Customer shall notify the Bank immediately and complete the loss report formality. If the Customer wishes to resume the use of any recovered Security Device or apply for a new Security Device, it shall bring identity documents and original chop and go to the Bank for the completion of the formality. The Customer must account for any unauthorised use of the Service before it completes the loss report formality. If the transaction is already processed by the Bank, it is deemed as made on behalf of the Customer. However, if the Bank fails to exercises due diligence of a good administrator for the control of information system or other reasons attributable to the fault of the Bank that

result in impersonation or misappropriation of the Security Device of the Customer, the Bank is liable for the loss.

(3) Effect of Transactions

Without prejudice to Clause 3(2) herein, the use of Security Device for a transaction shall be deemed to have been made on behalf of the Customer, and the Bank shall not be required to verify whether or not such transaction was authorised.

13. Effect of Electronic Instructions / Communications

(1) Unless it is otherwise provided according to law, the Bank and the Customer agree to the use of Electronic Messages or Communications (including transfer instructions of pre-defined transfer account, batch transfer, remittance transfer, batch remittance, bill collection file transfer, and application, modification, or termination of business relationships) in relation to transactions made available over the Service. In this regard, Electronic Messages or Communications shall be deemed to have been issued on behalf of the Customer if related agreed identification methods such as digital signature, User Code, and User Password are verified.

(2) Without prejudice to the generality of the foregoing:

i. the Customer does not need to complete a hard copy of the usual deposit, transfer or withdrawal receipt or remittance notice for the Bank to effect such deposit, withdrawal, transfer or remittance as instructed by the Customer over the Service;

ii. the Customer cannot claim that any Electronic Messages or Communications are invalid, false or unauthorised due to lack of written document or signature in any mediation, arbitration, court, administrative or other dispute resolution proceedings.

14. Receipt of and Response to Electronic Instruction / Communication

(1) When the Bank receives any instructions or communications over the Service, the Bank will verify that the person giving the instruction or communication is the Customer by reference only to the use of the relevant security information and Security Device. After receiving an Electronic Message or Communication that contains a digital signature or identification as agreed by the Bank and the Customer (except where such communication constitutes an enquiry on any matter), the Bank shall provide a webpage with a summary of the transaction requested by the Customer for reconfirmation by the Customer and then immediately undergo checking and processing, and notify the Customer of the results of checking and processing with Electronic Messages or Communications.

(2) Once the Bank has verified such instruction, the Bank shall be entitled to regard such instruction as irrevocable, valid and binding on the Customer. The Customer authorises the Bank to act upon all such instructions and hereby accepts all responsibility for the accuracy of information contained in such instructions. Any Electronic Messages or Communications received by the Bank or the Customer from each other is deemed not sent if the identity of the Bank or the Customer, or the content of such instruction or communication, is unidentifiable. Each party shall notify the other if the identity of the sender can be confirmed but the content is unidentifiable.

(3) The Bank is not deemed to have received any instruction or communication until the Service indicates that such instruction or communication has been received by the host system of the Service.

15. Non-execution of Electronic Instruction / Communication

(1) The Bank shall not be obliged to carry out any instruction or communication received over the Service, and may refuse act on any instruction or communication without liability. Without prejudice to the foregoing, the Bank may refuse to execute any instruction or communication received over the Service where:

i. The Bank determines that such instruction or communication is unclear or incomplete;

ii. The Bank has any reason to suspect the authenticity or accuracy of the instruction;

iii. The Bank has reason to believe that it may be in violation of any applicable law or regulation if it complies with or act on the instruction or communication;

iv. The Bank has reason to believe there is a breach of security or misuse of any Security Device;

v. The Bank is unable to deduct the required fees from Customer's account(s) for the account of the Customer.

(2) If the Bank decides not to execute or act on any electronic transaction or communication, the Bank shall use its reasonable commercial endeavours to notify the Customer of the situation and its reason for non-execution in accordance with the Bank's practice from time to time. Upon receiving such notice, the Customer may confirm the authenticity or accuracy of any instruction or communication, and the Bank shall be entitled (but not obligated) to act on such instruction or communication.

(3) The Customer is responsible for any errors or inaccuracies in any instructions or communications over the Service.

16. Time for Processing of Instructions / Communications

(1) The Customer's instructions or communications received by the Bank are automatically processed by the Bank computer systems. The Customer may not withdraw, revoke, or modify an instruction or communication after it has confirmed the accuracy of its content according to the reconfirmation mechanism provided by the Bank according to Paragraph 1 of Clause 14 herein and has sent such confirmation to the Bank. However, in relation to any pre-scheduled transaction that has not taken place, the Customer may withdraw, revoke, or modify the relevant instruction within such period specified by the Bank (currently, one Business Day before the pre-scheduled transaction day). If an instruction or communication is sent via the network to the Bank past the service hours for automatic processing, the Bank shall notify the Customer via an electronic communication or on the transaction screen that the transaction will not be processed, or will be processed on the next Business Day.

(2) If the instruction for a pre-scheduled transaction is sent to the Bank prior to the designated transaction date and the designated transaction date is not a Business Day, then such instruction will automatically be processed on the next Business Day. If the Bank's business or computer systems have been disrupted owing to any events of force majeure (such as typhoon, earthquake, etc), the pre-scheduled transaction will not be processed.

17. Checking the Transactions

(1) After completing the processing of each Global MyB2B transaction as instructed by the Customer, the Bank shall notify such transactions to the Customer (whether by sending an Electronic Message or Communication, instant display, or other method agreed with the Customer).

(2) The Customer must check whether each transaction as notified by the Bank is correct. If the Customer finds any error in the transaction content or transaction statement, it shall notify the Bank to investigate within 45

days from the date of receiving the statement.

(3) Upon receiving the Customer's notice, the Bank shall investigate immediately and reply in writing the findings or result of investigation within 30 days from the date of receiving the notice. Records of transactions as maintained and stored in the Bank's computer systems shall be deemed to be conclusive unless such records are proven to be inaccurate to the satisfaction of the Bank during such investigation.

(4) In addition to the foregoing, the Customer must carefully examine each statement of account to ensure that the transactions made through the Service are properly effected and there has been no unauthorised transaction. The Bank will not issue any separate statement(s) of account in respect of transactions effected using the Service.

18. Fees

(1) The Customer agrees to pay service fees and other published fees according to the agreed fee schedule starting from the date of using the Service, and hereby authorises the Bank to deduct such fees automatically from any of the Customer's account(s).

(2) If the fee schedule in the preceding paragraph is subsequently adjusted, the Bank shall publish such change on the Bank's website 60 days prior to the adjustment effective date and inform the Customer of such fee adjustment by email. The adjustment effective date shall not be earlier than the first day of the next year following the year of announcement and notice.

(3) Where the fee adjustment in Paragraph 2 hereof pertains to fee increase, the Bank shall offer the Customer an option (whether on its webpage or otherwise) for the Customer to indicate whether it is agreeable to the fee increase. Where the Customer did not indicate its consent before the date the fee adjustment takes effect, the Bank may suspend all or part of the Customer's access to or use of the Service starting from the adjustment effective date, and promptly reinstate the availability of the Service to the Customer if the Customer agrees to the fee adjustment later on.

(4) All fees payable by the Customer to the Bank do not include applicable taxes which shall be borne by the Customer. The Customer shall pay separately for such taxes and hereby authorise the Bank to deduct such taxes automatically from any of the Customer's account(s).

19. Errors in Instructions or Communications

(1) Where there is any error in any instruction or communication sent by the Customer for reasons not attributable to the fault of Customer, the Bank shall use its reasonable commercial endeavours to assist the Customer in making correction and provide other necessary assistance.

(2) Where any error in any instruction or communication sent by the Customer is attributable to the fault of the Bank, the Bank shall use its reasonable commercial endeavours to make the relevant correction immediately upon learning of the mistake, and notify the Customer via electronic communication over the Service or in any other manner as determined by the Bank from time to time. The Customer agrees to provide the necessary assistance.

(3) Where any error in any instruction or communication sent by the Customer is attributable to the fault of Customer, and the error pertains to the Customer making a mistake in the bank code, the account number, the amount to be transferred, the account from which funds are to be deducted or the account to which funds are to

be transferred, the Bank shall use its reasonable commercial endeavours to take any or all of the following action immediately upon receipt of notice from the Customer:

i. Provide details and relevant information on the transaction in accordance with applicable laws and regulations;
ii. Notify the transferee bank to render assistance; and
iii. Reply to the Customer regarding the handling of the situation.

20. Security of Information Systems

(1) Each of the Bank and the Customer shall use reasonable commercial endeavours to safeguard the security of the relevant information systems to prevent illegal access to such systems, or the unauthorised acquisition, alteration or destruction of transaction records and/or the Customer's personal data.

(2) The Bank shall use its reasonable commercial endeavours to ensure that the Customer transactions are secured, including the installation of security features. Provided that the Bank has taken such steps and has not been grossly negligent or fraudulent, the Bank will not be responsible for any loss or damage that the Customer may incur in the event unauthorised transactions are effected on the Customer's accounts, even if the Customer has complied with these Terms and observed the security measures implemented by the Bank. For the avoidance of doubt, the Bank is not responsible for the consequences of any virus or other matters which may adversely affect the Customer's hardware or software.

21. The Bank's Liability

(1) The Bank does not warrant or guarantee the right to access and use the Service. The Customer may experience interruptions and difficulties accessing or using the Service (including access to the Bank's website, portal and contents) from time to time. The Bank does not represent or guarantee that the Service, its website, portal and contents will be free from errors, viruses or interruptions. The Customer acknowledges and agrees that its access may be affected by outages, faults or delays which may be caused by technical difficulties, the Customer's or a third party's software, equipment or systems, traffic, infrastructure failure or actions by third parties. The Bank may also alter, interrupt, suspend or deny access to all or any part of the Service, its website, portal and contents at any time for any reason the Bank thinks fit, without any prior notice.

(2) If the Bank's website or portal experiences any breakdown or interruption, corruption of data or any other form of system failure resulting in the Customer not being able to access or use the Service effectively, then, upon request from the Customer, the Bank shall use its reasonable commercial endeavours to reinstate the Service as soon as reasonably practicable. The Bank shall not be liable for any damage or loss the Customer may suffer as a result of such breakdown, interruption, corruption of data or any other form of system failure.

(3) The Bank's website or portal may contain links or references to third party websites for the Customer's convenience. The Bank is not responsible for the availability or content of any such third party website and any links or references is not an endorsement by the Bank of the third party website, its contents or its provider.

(4) All terms implied by law relating to the functionality or use of the Service are hereby excluded to the full extent permitted by any applicable laws.

(5) Unless any loss, damage or expense incurred or suffered by the Customer has been caused by the Bank's gross negligence, fraud or deliberate misconduct, the Bank will not be responsible for any such loss, damage or

expense. Without prejudice to the foregoing exclusion, the Bank's liability for any breach of any conditions, warranties or rights for any reason whatsoever will (to the extent allowed by law) be limited to the supply of the Service or the cost of having the Service reinstated, as the Bank may determine conclusively.

(6) The Bank is not liable in any event for any indirect or consequential loss, damage or expense that the Customer may incur or suffer arising from its access to or use of the Service.

22. Treatment of Force Majeure Events

If any transaction (including any transfer or remittance operation) cannot be performed within the usual time-frame (on the same Business Day or otherwise) due to computer failure, network interrupts, or other reasons that are not attributable to the Bank, it will be processed as follows:

(1) The Bank can cancel all purported transaction (including any transfer and remittance operation), correct the relevant transaction records and refund any deductions to the relevant accounts of the Customer.

(2) The Customer can re-apply for transfer or remittance on the next Business Day.

23. Retention of Records

(1) The Bank and the Customer should retain the records of all Electronic Messages or Communications on transaction instruction and ensure the truthfulness and integrity of such records. Notwithstanding the preceding, records of transactions as maintained and stored in the Bank's computer systems shall be deemed to be conclusive unless such records are proven to be inaccurate to the satisfaction of the Bank during any investigation (whether based on Customer's records or otherwise).

(2) The Bank shall exercise due diligence of a good manager for the retention of records mentioned in the preceding paragraph and retain the records for at least 5 years or longer if so required by any applicable law.

(3) The reference to Electronic Messages or Communications on transaction instructions mentioned in the preceding paragraph include all documents relating to the transfer of funds or directly affecting the interests of the Customer, such as transfer, remittance, various payments, tax payments, payments on behalf of the Customer, and pre-scheduled transfers.

24. Modification of Service Functions and Terms

(1) The Customer acknowledges and agrees that:

i. The banking and other services made available through the Service are subject to limitations, and that the Bank may at its discretion add to, modify, restrict, suspend or terminate such services at any time.

ii. The Customer shall be bound by the Bank's update or amendment to these Terms and any applicable policies, rules or regulations of the Bank in relation to the use of the Service (whether in relation to the launch of new products or related service items, or otherwise).

(2) The Customer agrees that the Bank may notify any revision to these Terms by written notice to the Customer or by publication on the Bank's website (in-lieu of specific notice to the Customer).

(3) The Customer shall be deemed to have accepted any revision to these Terms if the Customer did not raise any objection in 7 days after receiving such a notice.

(4) However if the change in these Terms concerns the manner in which the Customer notifies the Bank of any breach of security procedures, the Bank shall notify the Customer at least 60 days in advance in writing or in

email to state the changes and the provisions before and after the change, and inform the Customer that it may raise objection before the change takes effect and that the Customer is deemed to accept the revision, addition or deletion if it did not raise any objection during said period of time.

(5) The Customer may change any of its customer or account information as well the designation of account(s) to be linked to the Service by completing and submitting to the Bank, such application form as the Bank may prescribe from time to time.

25. Termination of Service

(1) The Customer may terminate its access to or use of the Service at any time by completing and submitting to the Bank, such application form as the Bank may prescribe from time to time.

(2) The Bank is entitled to cancel the use of any security information or any Security Device and/or to withdraw, restrict or suspend the Service (whether in whole or in part) and/or terminate the Service under these Terms at any time when the Bank consider necessary or advisable to do so in its discretion without notice and the Bank shall not be liable to the Customer for any loss or damage resulting from or in connection therewith. The Bank shall nevertheless use its reasonable commercial endeavours to give the Customer not less than 30 days' prior notice in writing if the Bank intends to modify these Terms or the provision of the Service, or the Customer's right to access and use the Service.

(3) Without prejudice to the foregoing, the Bank shall be entitled to terminate the Customer's right to access and use the Service immediately if:

i. The Customer transfers or purports to transfer any of its rights or obligations under these Terms to a third party without the consent of the Bank.

ii. The Customer is insolvent, has filed or is subject to any winding up, judicial management or debt restructuring proceedings under applicable laws.

iii. The Customer has breached any provision of these Terms and has failed to remedy such breach after the Bank has demanded remedial action or requested performance within a given time period.

iv. The Customer violates related regulations of certificate issuing organisation.

26. Online Time Deposit Service

(1) When the Customer conducts time deposit service online, money can only be transferred from the Customer's demand deposit account at the Bank into the Customer's time deposit account of the same currency. When the term of the deposit is terminated early or upon maturity, the money can only be transferred from the Customer's time deposit account into the Customer's original demand deposit account when the time deposit term was settled (hereinafter referred to as "Settlement Day"). Settling and termination of time deposit can only be conducted during normal service hours of the Bank, and the term of the deposit cannot be modified or cancelled once it is settled.

(2) When the Customer applies for this service, the currency for deposit is subject to the listed currencies of the Bank, the term of the deposit is subject to the listed terms of each currency, and the interest rate is subject to listed interest rates of online foreign exchange time deposit disclosed by the Bank's online banking.

(3) The 4 ways for matured capital and interest are available for the Customer: capital and interest are transferred into original demand deposit account upon maturity without renewal, interest is transferred into original

demand deposit account upon maturity and renewal for capital, renewal for both capital and interest with the original term, interest in transferred into original demand deposit account every month and renewal for capital. Physical deposit certificate will not be issued for this service. Therefore, functions such as pre-scheduled transfer deposit slip, pledge, creation of pledge, etc are not provided.

(4) If an early termination of a deposit is made, it can only be processed on Global MyB2B with agreed certificate or identification method. Capital and interest can only be transferred into original demand deposit account. Early termination cannot be accepted on the Settlement day.

(5) The applicable physical chop for online time deposit service is the same as the chop for original demand deposit account. It is applicable when the termination cannot be realized through Internet banking and has to be processed at the counter (for example, due to failure of computer system or the deducted account has been written off).

27. Outward Transfer Remittance Service

(1) When the Customer conducts outward transfer remittance online, the account for outward transfer can only be the pre-defined demand deposit and demand savings deposit accounts of NTD or foreign exchange demand deposit account stated in the application submitted by the Customer in such form as the Bank may precribe from time to time.

(2) Unless otherwise indicated by the Customer, the Customer authorises the Bank or correspondent bank of the Bank to perform outward transfer remittance by any way or method deemed appropriate by the Bank, and the Customer further authorises the Bank to designate any foreign correspondent bank as settlement bank or intermediary bank. If the mistake is caused by foreign settlement bank or intermediary bank, the Bank will not be responsible, whether such bank was specified by the Customer or designated by the Bank in its discretion (unless there was gross negligence, fraud or deliberate misconduct by the Bank). The Bank shall assist to trace and inquire per the Customer's request. The required cable fee and fees collected by the relevant foreign bank shall be borne by the Customer. The Bank can request the Customer to make part of the payment before processing.

(3) The Bank is not responsible for delayed or undelivered remittance which was caused by any matter beyond the control of the Bank. The required cable fee and fees collected by the relevant foreign bank shall be borne by the Customer when Bank assists with the procedure of remittance refund or transfer owing to the above reason.

(4) The Customer agrees that when outward transfer remittance is settled or transferred by the relevant foreign bank, the payee is responsible for fees deducted from the remittance by settlement bank and intermediary bank in accordance with conventions of local bank. The Customer will not have any objection to the amount of such fees or the deduction thereof. The Customer agrees that the foreign settlement bank, which was assigned by the Bank, can make the payment to payee's account with original currency or local currency exchanged by current day exchange rate. The Customer will not have any objection to the relevant exchange rate.

28. Notification of Transactions

(1) The Customer authorises the Bank to provide notifications of **Global MyB2B** transactions to such email addresses, fax numbers and telephone numbers that the Customer notifies to the Bank from time to time (whether by email, fax or otherwise).

(2) The Customer acknowledges and agrees that:

i. it consents to the Bank's dispatch of confidential information which is not encrypted and may include details of the Customer's account information to such email addresses, fax numbers and telephone numbers;

ii. it has the sole responsibility to verify the accuracy and authenticity of such email addresses, fax numbers and telephone numbers;

iii. the sending of any notification or receipt of the same may be delayed or prevented by matters beyond the Bank's control;

iv. it will undertake all risks of any wrongful information disclosure (whether owing to unauthorised access to such emails, devices or otherwise), and shall not hold the Bank responsible in any way;

v. it has the sole responsibility to enable notification alerts on any device that is used to receive notifications of **Global MyB2B** transactions, to opt to receive all notifications of **Global MyB2B** transactions for all outgoing transactions made from the Customer's accounts, and to monitor such notifications sent to such email addresses, fax numbers or telephone numbers. The Bank may assume that the Customer will monitor such notifications without further reminders or repeat notifications;

vi. if its preferred notification threshold amounts result in fewer notifications, its ability to monitor unauthorised **Global MyB2B** transactions, and its liability for any unauthorised **Global MyB2B** transactions may be affected and it accepts liability for any losses arising from unauthorized **Global MyB2B** transactions due to its recklessness;

vii. it disclaims all claims against the Bank for any damage or loss that it may incur or suffer in connection with the notification of **Global MyB2B** transactions (whether arising directly or indirectly from (a) non-delivery or the misdirected delivery of any notification; (b) the inaccurate or incomplete content in any notification; (c) reliance on or use of the information provided in an SMS Alert for any purpose; or (d) any third party, whether authorised or not, obtaining account information contained in the notification by accessing the relevant email addresses, fax and/or telephone.

(3) The Bank reserves the right to terminate its notification services by giving prior written notice to the Customer.