E.SUN Bank Singapore Branch eBanking Service Agreement

The Applicant hereby applies for E.SUN eBanking (hereinafter "internet banking") services. After consultation with E.SUN Commercial Bank, Singapore Branch (hereinafter "the Bank"), the Applicant agrees to the following terms and conditions, the Applicant having thoroughly reviewed and understood them completely. The Applicant also understands that the internet banking service is developed by the Information System Division of the E.SUN Bank Taiwan main branch as commissioned by the Bank and the server is set up in the Division. The Applicant hereby agrees that the relevant information of the business transactions with the Bank under the Applicant's Customer ID can be inquired by Applicant (or Designated Member), and transfers and remittances can be conducted by the Applicant (or Designated Member) through internet banking. If there are any additions, deletions or changes to the service contents, the Bank will announce such changes at its operating premises or its website. The Applicant hereby agrees to conduct its business in accordance with such changes.

Article 1 Bank information

I. Name of bank: Singapore Branch, E.SUN Commercial Bank

II. Customer service hotline: +65-6533-1313

III. E.SUN eBanking Address: https://gib.esunbank.com/SG/

IV. Address: Kindly refer to E.SUN Bank Singapore Branch website: https://www.esunbank.com/zh-tw/business/corporate/overseas-branch/singapore

V. The visitor message board: https://www.esunbank.com/zh-tw/about/services/customer/message-board

Article 2 Applicability of terms and conditions

The "Standard Terms and Conditions Governing Accounts" are the common agreement of the Agreement. Unless otherwise agreed upon in the Agreement, the "Standard Terms and Conditions Governing Accounts" shall be complied with. The Agreement shall not contradict the "Standard Terms and Conditions Governing Accounts".

The Agreement serves as a common agreement for internet banking services. It applies to all services offered under the Agreement unless otherwise stated in the contract of respective internet banking services. Respective internet banking service contracts shall not contradict the terms of the Agreement.

Any product or service of the Bank handled via internet banking shall in comply with the respective agreement regarding the rights and obligations of the product or service between the Applicant and the Bank, and the Agreement shall not apply.

Article 3 Definition

"Internet banking services": Various financial services offered by the Bank that the Applicant can access from the Applicant's computer through internet connection with the Bank, without visiting the Bank in person.

"Electronic documents": Any text, audio, image, video, symbol, or other type of data transmitted by the Bank or by the Applicant over the internet, which has been arranged in electronic or other not directly recognizable format, but that can be processed electronically to convey meaning.

"SoftToken": Multi-factor device binding verification function allows users to use the bound mobile device and the password from a SoftToken password slip to conduct verification on the server end. After the verification is complete, users may use the transaction verification password of their choice to conduct identity verification for transactions.

"SoftToken Number": The only serial number on the SoftToken password slip given to the Applicant by the Bank.

"Digital signature": The process of converting electronic documents into a certain length of digital information using mathematical algorithms or other methods, and encrypting them with the signatory's private key. The digitally signed message can be authenticated using a public key.

"e-Certificate": Electronic documents that are signed with a digital signature by the certification authority for verifying the identity of an Applicant for certification and providing digital proof of the actual possession of a matching set of public and private keys.

"Original token device password": The dedicated password for the activation of saving and processing of the digital signature mechanism.

"Public key": These digital data are used to encrypt electronic documents and validate the signatory's identity and the digital signatures.

"Private key": The part of paired digital data retained by the signatory; these digital data are used to create a digital signature and decrypt ciphered electronic documents.

"Security control equipment": The security control equipment applied by the Applicant to the Bank. "Currently, the device is either SoftToken or FXML." The Applicant's maximum amount and other rights and obligations for transfers via internet banking are all based on the application of Security control.

"Applicant Account": Deposit accounts (excluding time deposits) that the Applicant identifies to the Bank, in writing or through the digital signature mechanism, as accounts for transaction related payments.

"Authorized personnel": The officer who is designated to manage user authorization and control or configure transaction processes on behalf of the Applicant in the internet banking environment.

"Service hours": Monday to Friday, 9:00 am to 3:30 pm, except for days when the Bank is closed in accordance with regulations or competent authority's orders. However, due to the nature of certain transaction services, their service hours are subject to the Bank's announcements on its website. The Bank may, after making an announcement, suspend internet banking services provided to the Applicant due to account settlement or service suspension of its computer systems.

"Automated services": Transaction services sent from the Applicant's computer to the Bank for payment after implementation.

"Designated member": The person designated by the Applicant to conduct internet banking business with the Bank within the scope of the authorization.

"At the counter": The Applicant conducts business at the counter of the Bank.

"Submission of Original": The Applicant submits the well-completed and signed designated original documents to the Bank by post.

Article 4 Mobile CEO+ APP Service

I. Mobile CEO+ APP services enable the Applicant to have access to various financial services made available by the Bank through logging in to Bank's internet banking platform via electronic means (such as: mobile device or other devices that can connect and access the internet.)

II. The Applicant has to be a member of the Bank's internet banking services in order to apply for Mobile CEO+ services. By applying for Mobile CEO+ services, the Applicant agrees to be enrolled as the Bank's Mobile CEO+ member, and is aware that the Bank prohibited the Applicant from modifying his/her device (such as: root, jailbreak, USD debugging, etc.) to log in and access the Mobile CEO+ APP services.

III. Mobile CEO+ APP services is to enhance the provision of the Bank's internet banking services, so the usage methods and services guideline are handled in accordance with the Terms and Conditions governing the use of the internet banking services。

IV. The Applicant may gain access to the internet banking services through the link of the Bank's official website (https://www.esunbank.com) or the software provided by the Bank (such as smart phone application software). The Applicant is to be solely responsible and liable for data leakage, losses and other consequences arising from or in connection with Mobile CEO+, in the event that the Applicant access Mobile CEO+ apart from the above-mentioned link or software provided by the Bank.

V. If the Applicant notices any suspected counterfeit, fraudulent or software purporting to be from Mobile CEO+ application, please contact the Bank immediately. It is the responsibility of the bank, on an on-going basis, to keep an eye out for suspicious counterfeit of Mobile CEO+.

Article 5 Website verification

Prior to using the internet banking, the Applicant shall first verify the E. SUN eBanking website: https://gib.esunbank.com/SG/ before using the internet banking services. For any question, please contact the Singapore Branch, E.SUN Commercial Bank. Service hotline: +65-6533-1313. Feedbacks or complaints may also be given via the visitor message board. After receiving a customer message or recommendation, the message will be sent to the dedicated staff based on the business type and be replied within a designated time frame. For more information, please see: https://www.esunbank.com/zh-tw/about/services/customer/message-board

The Bank shall exercise due diligence in the detection of fake websites.

Article 6 Internet for the connection

The Bank and the Applicant both agree to transmit and receive electronic documents over the designated secured Internet.

The Bank and the Applicant shall enter the service agreements with their respective Internet service providers to secure their own rights and obligations; both parties shall bear their own expenses incurred for accessing the Internet.

Article 7 Receiving and responding to electronic documents

Upon receiving a digital signature or any electronic document agreed upon by the Bank and the Applicant as an appropriate means of identification, the Bank shall prompt for the Applicant's confirmation by displaying key information on the webpage (except for inquiries) before proceeding with verification and execution. The Applicant shall be notified of the results of the verification and execution by the method agreed upon between the two parties.

In circumstances where the Bank or the Applicant is unable to determine the identity or the content of electronic documents sent by the other party, the electronic documents shall be considered to have never been sent in the first place. However, where it is possible for the Bank or the Applicant to ascertain the other party's identity, the receiver shall notify the sender of the fact that the message contents were unidentifiable using methods agreed upon by both parties.

The Bank may reject communication requests that do not comply with procedures or suggest reasonable doubt as to the contents, authorization, or source. The Bank shall also notify the Applicant of the rejected data by phone call or other methods.

Article 8 Non-execution of electronic documents

The Bank may refuse to execute an incoming electronic document if it meets any one of the following descriptions:

I. Where the Bank has reasonable doubt as to the authenticity of the electronic document or the correctness of the instructions;

II. Where the Bank might be at risk of violating laws or regulations should it choose to process the electronic document;

III. Where the Bank is unable to debit from the Applicant's account for the amount payable, for reasons that are attributable to the Applicant.

Should the Bank choose to forgo execution of electronic documents due to the above reasons, the Bank shall provide the Applicant with reasons for the non-execution. The Applicant may call the Bank for confirmation after being notified.

Article 9 Application for SoftToken

To use SoftToken for transactions on the Bank's internet banking platform, the Applicant agrees to the following terms:

I. The Applicant should access the service through the link provided on the official website of the Bank (http://www.esunbank.com) or the application (such as the smart phone application) provided by the Bank. If data leakage or other damage is caused while the Applicant accesses Mobile CEO+ through methods other than via the aforementioned link on the website or software of the Bank, the Applicant will be held accountable for any consequences ensuing.

II. Applicability of SoftToken: The Applicant understands and agrees that classifications and definitions of applicability are subject to the Bank's regulations.

III. Functions of SoftToken: The Applicant agrees that for the application of the SoftToken password slip issued by the Bank, login and verification shall be conducted through the method designated by the Bank or relevant fees shall be paid.

IV. The Applicant agrees that the SoftToken password slip applied for shall be provided through the method designated by the Bank.

V. The Applicant agrees to read thoroughly the information provided by the Bank during the application as well as the information on the Bank's website. The Applicant agrees to comply with all the requirements stated in such information and the Bank's regulations.

VI. The Applicant may not demand the Bank to refund the fees for the SoftToken password slip if the Applicant applies for the annulment of SoftToken for any reason during the usage of SoftToken.

VII. The Applicant agrees to safeguard the issued valid SoftToken. During the usage, if SoftToken is damaged for any reason, the Applicant may reapply to the Bank and pay relevant handling fees.

VIII. The Bank reserves the ultimate right of approval of the SoftToken application.

IX. After verification in the Bank's system, the SoftToken held by the Applicant shall be deemed equally valid as the Applicant's seal, signatures or other method agreed upon.

Article 10 Loss or malfunctioning of SoftToken

Upon discovering that the SoftToken password slip applied for to the Bank is lost or malfunctioning, the Applicant shall immediately notify the Bank and apply for the suspension of SoftToken function in the internet banking. Transactions conducted by the Applicant before suspension of SoftToken are considered valid instructions from the Applicant, for which the Bank bears no liability.

In cases where the Applicant is unable to provide the SoftToken Number for the lost SoftToken password slip, and the Bank is therefore unable to suspend the specific SoftToken Number, the Applicant authorizes the Bank to suspend all the passwords under the specific user code to protect the Applicant's interests. However, the Bank is not liable for any inconvenience or loss caused due to such suspension.

In cases where the Applicant finds out the lost SoftToken password slip or is sure that the slip functions are recovered after notifying the Bank of the loss or malfunctioning, the Applicant shall visit the Bank to reinstate the slip. If the SoftToken function has already been canceled, it cannot be reinstated. In this case, the Applicant shall apply to the Bank for a new SoftToken password slip.

Article 11 Electronic certificate application

To use a digital signature for transactions on the Bank's internet banking platform, the Applicant agrees to the following terms:

I. Certificate application and renewal: The Applicant agrees to apply for an electronic certificate issued by an institution specified by the Bank and pay the fees incurred by the method instructed by the Bank, or authorize the Bank to collect the fees directly from the Applicant's designated account when the application or renewal is processed.

II. The Applicant agrees that the password slip for the electronic certificate shall be provided by the Bank via the specified method.

III. Applicability of certificate: When applying for certificates, the Applicant shall designate the specific applicability for each individual certificate with the Bank. A certificate is valid only within the scope specified by the Applicant Classifications and definitions of applicability are subject to the Bank's regulations.

IV. The Applicant agrees to read thoroughly the information provided by the Bank and the certification authority during the application as well as the information on the Bank's website. The Applicant agrees to comply with all the requirements stated in such information and the Bank's regulations.

V. If, for any reason, the Applicant applies to cancel the certificate while it is still valid, the Applicant shall not request the Bank to refund the fees related to the certification.

VI. The Applicant agrees to safeguard the issued valid electronic certificate. During the usage, if the certificate is damaged for any reason, the Applicant may reapply to the Bank and pay relevant handling fees.

VII. The Bank reserves the ultimate right of approval of the certificate application.

VIII. After verification in the Bank's system, the electronic certificate held by the Applicant shall be deemed equally valid as the Applicant's seal, signatures or other method agreed upon.

Article 12 Loss of electronic certificate

The Applicant is aware that the electronic certificate applied for is issued by a certification institution (including but not limited to TAIWAN-CA) approved by the competent authority and that the certificate is saved in a carrier. Upon discovering that the carrier is lost, the Applicant shall immediately notify the Bank and apply for the suspension of the certificate via internet banking or at the counter of the Bank. Transactions conducted by the Applicant before the suspension of the certificate are considered valid instructions from the Applicant, for which the Bank bears no liability.

In cases where the Applicant is unable to provide the serial number of the certificate on the lost carrier, and the Bank is unable to suspend the specific certificate, the Applicant authorizes the Bank to suspend all the certificates under the specific user code to protect the Applicant's interests. However, the Bank is not liable for any inconvenience or losses caused due to such suspension.

If the certificate is later found after notification of loss to the Bank, the Applicant should visit the Bank itself to reinstate the certificate; If the certificate has already been canceled, the certificate cannot be reinstated. In this case, the Applicant shall apply to the Bank for a new certificate.

Article 13 Fees

Starting from the first day of using the services, the Applicant agrees to pay application fees for the SoftToken password slip or certificate, service fees, handling charges and Swift / Mail fees, etc., according to the standard rates stipulated by the Bank, and authorizes the Bank to collect all fees and charges from the Applicant's account.

In cases where the aforementioned rates are adjusted after the signing of the Agreement, the Bank shall announce the adjustments thirty days before the day of the adjustment in the Singapore Branch section on the Bank's website notifying the Applicant that the Agreement can be terminated by Applicant within the time frame. If the Applicant does not terminate the Agreement within the time frame, the Applicant shall be deemed as consenting the relevant fee adjustments.

Taxes payable by the Applicant shall be paid according to the tax laws and regulations related to the taxes payable by the Applicant of the Agreement and the Applicant authorizes the Bank to directly deduct the payment from the Applicant's account.

Article 14 Installation of software/hardware at the Applicant's side and associated risks

The Applicant shall install all computer software, hardware, and security-related equipment required to access the services offered under the Agreement. The Applicant shall bear all costs and risks associated with the installation.

Where the software, hardware and documents in Section 1 of Article 13 are provided by the Bank, the Bank only agrees Applicant to use within the scope of the services, and such software, hardware and documents shall not be transferred, borrowed, or in any other way given to a third party.

The Applicant is liable for any damages ensuing from the improper use or behavior infringing the intellectual property right or other rights of the Bank or third parties.

If the Applicant needs to install other software or hardware in order to run the software/hardware provided by the Bank due to computer operational requirements, the Applicant shall follow the installation guidelines provided by the Bank and bear the costs and possible risks involved.

Article 15 Applicant's connection and responsibility

The application or changes of the email are subject to the Bank's regulations as follows:

I. The Applicant understands and guarantees that the email address retained or changed with the Bank is indeed used by the Applicant. Furthermore, the Applicant agrees that the Bank is entitled to conduct the email sharing checking, i.e. to check whether the aforementioned email address is the same as other customers' email address retained with the Bank for the purpose of protecting the Applicant's rights. If they are the same, the Applicant agrees that the Bank may confirm the reason for the same email address with the Applicant and keep the relevant records.

II. The Applicant's email which will be retained or changed by the Bank shall be deemed valid after the email verification is completed, and the period of validity for the Bank's email for verification is 72 hours after the verification email sent by the Bank. The Applicant agrees to cooperate in completing the email verification of the Bank, and understands that the aforementioned email verification mechanism must be completed (such as clicking the email verification link sent by the Bank), so that the retention or modification procedures of the email address can be completed. If the aforementioned verification mechanism is not completed within a certain period of time, the Applicant is willing to re-execute the retention and modification procedures of the email address.

III. The Applicant agrees that for the first application of the internet banking services, the users are able to login eBanking system only after completing email effective verification, and for the eBanking existing customer who apply for changing email, the email will not be updated by the Bank if the email verification is not completed. The bank will use the retained email address as notification before email verification can be completed.

For the application of standard internet banking services, original password slips (including the reapplication after the cancellation of access rights), SoftToken password slips, electronic certificates, carriers and their password slips, the signature(s) of authorized persons of Applicant shall be kept on the application form, which bind on all of the accounts under Applicant; When Applicant applies for transfer services of internet banking, the signature(s) of authorized signatories of Applicant shall be kept for Applicant's application for the rights and obligations of the designated Applicant Accounts.

The user name and password the Bank provides to the Applicant can only be used for the first login. The Applicant should change the user name and password before accessing to other services. The Applicant may then change the user name and password when necessary. The Applicant shall also change the initial passwords of SoftToken, electronic certificates and carriers before using the account. Password changes of this service should follow the rules below:

I. For an Applicant who has not activated the licensing, after 5 consecutive incorrect entries of the internet banking username, the system will automatically suspend the user's authority to access the internet banking services. The authority will be re-activated the next day;

II. After 5 consecutive incorrect entries of password or upon the Applicant's failure to login and use the services for the first time within 30 days of the application, the system will automatically suspend the Applicant's authority to access the internet banking Services. The Applicant shall apply for resetting the password to the Bank before continuing to use the services.

III. After 5 consecutive incorrect entries of the carrier password, the system will automatically suspend the user's authority to access the carrier. The Applicant shall apply for resetting or reinstating the password to the Bank before continuing to use the services.

IV. The Applicant agrees that when the service has not been used for one year, the Bank may terminate the service.

V. After accessing rights are canceled, if the Applicant needs to use the service again, the Applicant should re-apply for it.

VI. To minimize risks, the Applicant shall from time to time change the passwords.

The Applicant is responsible for safekeeping the initial user names and passwords provided by the Bank, relevant documents, self- designated user names and passwords, SoftToken transaction verification passwords and carrier passwords.

For the application of SoftToken, the Applicant shall first download and open the Mobile CEO+ APP to begin binding the mobile device. Other operational matters should be in accordance with the following rules:

I. Each mobile device can only be bound to one SoftToken Number.

II. After 5 consecutive incorrect entries of the SoftToken password slip activation code or upon the Applicant's failure to login and use the services for the first time within 30 days of the application, the system will automatically suspend the Applicant's authority to access the internet banking services. The Applicant shall reapply to the Bank before continuing to use the services.

III. When Applicant conducts transaction verification via the SoftToken bound transaction verification password, after 5 consecutive incorrect verifications, the system will automatically suspend the Applicant's accessing right, and the Applicant shall reapply to the Bank before continuing to use the services.

IV. In cases where the Applicant changes the device or reinstall Mobile CEO+ for any reason, the SoftToken originally bound to the device shall automatically become invalid. If the Applicant wishes to continue using SoftToken, the Applicant shall reapply to the Bank and bind the function before continuing to use it.

Article 16 Billing date

Transactions conducted by the Applicant before the Bank's cut-off time are processed as same day transactions, and those are conducted after the cut-off time are processed on the next business day.

Article 17 Provisions on internet banking authorization

The Applicant may authorize its company staff (hereinafter called "authorized staff") to use the Bank's internet banking services.

The Applicant shall apply to the Bank in advance for the use of the internet banking authorization function. The Applicant shall use the authorization function provided in the Bank's internet banking services to authorize the authorized staff to use the Bank's internet banking services within the agreed scope.

The authorized staff's use of the Bank's internet banking services shall carry the same effect as if such services were used by the Applicant.

The Applicant shall be solely responsible for all losses incurred as a result of the Applicant's and/or authorized staff's negligence, improper use or improper management with respect to the use of internet banking services. The Bank shall not be held liable.

Article 18 Terms for internet banking transfer

Each designated Applicant Account shall be designated by the Applicant prior to using the internet banking transfer service.

The Applicant shall designate the designated Applicant Accounts for this service and the daily limited transaction amount of the Applicant Account in writing to the Bank; The Applicant may also designate the Beneficiary Accounts for the Applicant Accounts in writing to the Bank. Applicant may notify the Bank in writing to authorize the designated member to use the services provided on this system to process tasks commissioned to the designated member.

The Applicant agrees that instructed transfer and payment transactions are processed by the Bank based on the authority and security status in the Bank's system at the time when the transaction data were transmitted to the Bank. In cases where the SoftToken or authorization certificate is about to be suspended or canceled at the time of the Bank processing the transactions, the transfer and payment transaction instructions approved by the service system before the suspension or cancellation of SoftToken or the certificate are still considered to be valid instructions.

The maximum amounts for transfers and remittances will be stated in Article 19.

Article 19 Internet banking remittance services

The Applicant shall designate each Applicant Account for the automated outward remittance services in the internet banking. The Applicant may also designate the corresponding Beneficiary Accounts for this service in writing to the Bank.

The daily maximum amount for outward remittance of each Applicant Account and the limitation of corresponding Beneficiary Account is based on the Security control equipment applied by the Applicant to the Bank. However, for the amounts transferred into time deposits, the Beneficiary Account does not need to be designated for the transaction. Newly designated Beneficiary Account shall become valid the day following the application. The Applicant Accounts, the corresponding Beneficiary Accounts and the daily limited transaction amount can all be designated by the Applicant in writing to the Bank. Transfers and remittances exceeding the limited amounts shall be conducted at the counter in the Bank, by Submission of Original or via other methods agreed by the parties.

When the Applicant's Security control equipment is SoftToken, the amount limits are as follows:

I. Each inward and outward remittance for the automated remittance services in the internet banking shall be designated by the Applicant.

II. The accumulated maximum amount for the outward remittances (including accounts of different currency under the same main account of the Applicant) on the same business day is limited to the equivalent of 700,000 SGD.

III. The Applicant may apply to the Bank for non-designated account remittance services. The maximum amount for each outward remittance of each Applicant Account is 25,000 SGD. The daily accumulated maximum amount of each Applicant Account is 50,000 SGD, and the monthly accumulated maximum amount of each Applicant Account is 100,000 SGD.

When the Applicant's Security control equipment is "electronic certificate," the amount limits are as follows:

I. The Applicant shall designate each Applicant Account for the automated remittance services in the internet banking. The Applicant may also designate the corresponding Beneficiary Accounts for this service in writing to the Bank.

II. The accumulated maximum amount for the outward remittances and remittances conducted within the Bank between different accounts of Applicant on same business day shall be decided by the Applicant and the Bank (in SGD).

The Applicant agrees that when the internet banking remittance services have not been used for one year, the Bank may terminate the non-designated account remittance services. After the cancellation, if the Applicant needs to use the services again, the Applicant should re-apply to the Bank.

When applying for an outward remittance online, the Applicant agrees that the Bank will transfer the remittance to the designated account via SWIFT. In cases where the transferred amount is seized or frozen by the Bank's nostro bank due to reasons such as the payee being listed as a member of a terrorist organization or the payee's country being listed as a sanctioned country, the Applicant unconditionally agrees to bear all losses, and the Bank shall not be held liable.

The Applicant agrees that the exchange rates applicable to this service are subject to the Bank's real-time board exchange rates or exchange rates as previously agreed with the Bank. If the Applicant fails to complete the transaction(s) as agreed or requests to cancel the agreed transaction(s), the Bank may charge the Applicant default penalties for any losses incurred.

The Applicant agrees to the commitment exchange rate for the services, which may be based on the board rate of Bank or the exchange rate negotiated with the Bank. If the transaction is not completed in accordance with the agreement or the transaction is cancelled, the Applicant shall indemnify the

Bank for its losses and default penalty.

The Applicant understands that the Bank is not responsible for reviewing or identifying the transaction nature or purpose for the processing of remittances. The Applicant shall verify and confirm the accuracy of the transaction data to prevent from losses.

When conducting transactions via internet banking, the Applicant promises to provide relevant supporting documents of the transaction when the Bank needs to verify the transaction purposes.

When the Applicant conducts transactions via internet banking, the Applicant shall do so within the Bank's service hours. The Applicant shall truthfully declare the purpose of each remittance when conducting remittances via internet banking. In cases of false or incorrect reporting, the Applicant is solely accountable for any consequences.

The Bank may charge the Applicant any additional fees incurred when executing this service and the Applicant should pay these fees immediately upon receiving the Bank's notification.

The Applicant agrees that when applying for online remittances, the application should be processed in accordance with the regulatory requirements of the competent authority.

In cases where the internet banking service is interrupted or suspended for any reason, the Applicant agrees to conduct the transactions at the counter during business hours, by Submission of Original or via methods agreed by the parties as alternatives of the internet banking services, and the Bank shall proceed to receive instructions and handle the applications. For any question, please contact the Singapore Branch, E.SUN Commercial Bank. Service hotline: +65-6533-1313, service fax: +65-6636-3113。 Feedbacks or complaints can also be accepted via the visitor message board. After receiving a customer message or recommendation, the message will be sent to the dedicated staff based on the business type and will be replied within a designated time frame. For more information, please see: https://www.esunbank.com/zh-tw/about/services/customer/message-board.

Article 20 Agreement on co-utilization of internet banking

For purposes of internal operations, the Applicant agrees to co-utilize the Bank's internet banking services with members designated by the Applicant and allow the designated members to access the Applicant's corporate internet banking account, using the designated members' Customer ID/UBN, to utilize specified services the Bank provides to the Applicant. The Applicant agrees that when it co-utilize the internet banking services with the designated members to conduct group or cross-border capital management, even if the designated members are not located in the same region as the Applicant, Applicant will make sure that the designated members are conducting transactions in accordance with local laws and regulations as well as the transaction requirements of the region where the Applicant is located in (such as amount limit or service hours).

The group and corporate relationship between the Applicant and the designated member shall be handled based on the Bank's current regulations. The Applicant agrees and warrants that all the declared matters upon the application for the service are not false, untruthful or concealed, and any change to the aforementioned declared matters is the Applicant's sole responsibility. The Bank does not have the obligation to verify the accuracy of the content or the truthfulness of the submitted documents. Any damage to the Bank or a third party arising thereof shall be the Applicant's sole responsibility.

When the designated scope of co-utilization of internet banking is account inquiries, users appointed by the designated members may process inquiries or downloads of the Applicant's account information on the Bank's corporate internet banking system, while the Applicant still retains the right to access the corporate internet banking services.

When the designated scope of co-utilization of internet banking is account transactions, users appointed by the designated members may process inquiries or downloads of the Applicant's account information on the Bank's corporate internet banking system. The Applicant also agrees to allow the designated members to approve the Applicant's transactions using security equipment. Meanwhile, the Applicant agrees to give up the rights to access the corporate internet banking services.

The Bank may terminate the co-utilization service by the Applicant's or the designated member's request without obtaining consent from the other party. The Applicant understands and agrees that if the designated member terminates the internet banking services, the Bank may also terminate the co-utilization service provided for the Applicant and the designated member.

The Applicant agrees that all instructions and transactions conducted by the designated members on behalf of the Applicant are held as the conducted by the Applicant, and as such require no further verification from the Bank. The Applicant also agrees to be accountable for all consequences incurred therein.

The Applicant agrees to actively and promptly notify the Bank and resubmit relevant documents when the relationship or commercial interest between the Applicant and the designated members changes, and agrees to provide the newest documents on the relationship or commercial interest based on the Bank's needs for periodic review. The Applicant understands and agrees that the Bank may terminate the co-utilization of internet banking services between the Applicant and the designated members if the Applicant fails to cooperate with and meet those requirements of the Bank.

The Applicant agrees that the supervisory institutions in the regions of the E.SUN Bank main branch and other domestic and overseas subsidiaries may access the Applicant's personal information provided for the use of the services to the Bank. The Applicant agrees and authorizes the Bank to provide such information to the supervisory institutions. Without obtaining the Applicant's consent or for legal requirements, the Bank may not provide the personal information provided by the Applicant to any third party other than those mentioned above or use it for purposes unrelated to the Agreement.

Article 21 Transaction verification

The Applicant shall check and verify the transaction results for errors after each transaction instruction is handled. Any discrepancy should be reported to the Bank within 45 days of the transaction completion for investigation. The Applicant agrees that the consensus shall be reached according to the records provided by the Bank and the confirmation of both parties.

The Bank shall compile a statement of transactions conducted in the previous month, and deliver it to the Applicant on a monthly basis using electronic documents or methods agreed upon by the two parties (statements may not be delivered for months where no transactions took place). For Applicant applied to co-utilization of internet banking services is deemed to have authorized the Bank to deliver the statements (including all accounts of Applicant) via methods agreed upon between the designated members and the Bank. The Applicant should verify all items listed in the transaction statement, and notify the Bank any errors found within 45 days after receiving the statement. The Bank shall conduct investigation upon receiving the Applicant's notification and inform the Applicant of the outcome of the investigation within 30 days after receiving the notification.

The Applicant agrees that the remittance transaction results may be notified to the Applicant via internet inquiries, internet statements or electronic messages from the Bank. (For failed deliveries for any reasons not attributable to the Bank, the results will not be re-delivered for that month.) The Applicant also agrees that the account balance and transaction details recorded in the Bank's system are final and undebatable.

Article 22 Responding to errors in electronic documents

If the Applicant encounters any errors in electronic documents of the services specified in the Agreement that are not attributable to the Applicant, the Bank shall assist the Applicant in rectifying the error, and the Applicant shall actively cooperate with the Bank for the rectification.

In the case of errors in electronic documents of the services specified in the preceding section that can be attributed to the Bank, the Bank shall make corrections immediately upon becoming aware of the errors, and, at the same time, notify the Applicant via electronic documents or by any other methods agreed by the Bank and the Applicant. The Applicant shall also actively cooperate with the Bank for the rectification upon receiving notification.

In the event that, during the use of the services, the Applicant transfers funds into the wrong account or in a wrong amount, such as by entering an incorrect bank code, account number, or amount, the Bank shall provide the following assistance immediately upon being notified by the Applicant:

I. Provide details relating to the transaction and relevant information to the extent permissible by law.

II. Notify the receiving bank for assistance.

III. Report the results.

The Applicant agrees to bear the responsibility for any losses, liabilities, or costs incurred due to the Bank's efforts in assisting the Applicant to recall, cancel or rectify the information or message or in providing other necessary assistance.

Article 23 Authorization and responsibilities associated with electronic documents

The Bank and the Applicant shall ensure that all electronic documents transmitted to the other party are legally authorized.

If the Bank or the Applicant discovers any misuse or theft of username or password, or any unauthorized conduct by a third party, the Bank or the Applicant shall promptly notify the other party by phone, in writing or by any other methods agreed by the parties to suspend the use of the service and take necessary precautions.

In the cases where the Applicant fails to prove that the Bank was promptly notified, any consequence arising from the third party's use of the service shall be the Applicant's sole responsibility.

Article 24 IT system security

The Bank and the Applicant are responsible for safekeeping electronic documents in their respective IT systems in order to prevent any third party from illegally entering the system or stealing, altering, or destroying any business records or information.

The Applicant should keep information of this service properly, with no attempt to destroy or transfer it for inappropriate use.

The Applicant shall be held liable for the damages incurred to the Bank or a third party arising from the viruses or other information security weaknesses found in the electronic documents uploaded by the Applicant.

Article 25 Obligation of confidentiality

Unless otherwise regulated by law, the Bank and the Applicant must ensure that the electronic documents exchanged with the other party and any information of one party obtained from the other party while using or offering the services under the Agreement are not disclosed to any third party, and nor can they be used for purposes unrelated to the Agreement. If the owner of the information has given consent to disclose such information to a third party, the third party must be made to comply with confidentiality requirements stipulated in this article.

If the third party referred to in the preceding section fails to comply with the duty of confidentiality, the Applicant will be deemed to be in breach of its obligations.

The Applicant understands that the internet banking service and the relevant accounting system are developed and maintained by the Information Technology Division of the Taiwan main branch as commissioned by the Bank. The Bank shall ensure that the Information Technology Division of the main branch has set up necessary security control measures for the storage and use of the customer information and transaction records to secure the confidentiality and completeness of the customer's data.

Article 26 Bank disclaimer

Where the Bank or the Applicant fails to perform obligations arising from the Agreement or fail to perform them on time, consequently causing damages to the other party, the party at fault shall be held liable for any damages arising thereof. However, this shall not apply in the case of force majeure.

Force majeure events refer to natural disasters, strikes, shutdowns, limitations imposed by government regulations, or any other events beyond the Bank's control.

The Bank is not responsible for processing information which is sent without following the required procedures. Moreover, the Bank is not liable for any errors, omissions, or repeated submission of information caused by the Applicant.

The Bank shall consider any applicable laws, regulations, templates, guidelines, notices, codes of conduct and common market practices, take reasonable and viable steps to ensure that sufficient security facilities are set up for the internet banking service related systems, and monitor relevant risks during system operation.

The Bank or any information provider does not guarantee or warrant that the internet banking services, information and reports are free from viruses or other issues that may damage the Applicant's hardware, software or equipment.

Unless otherwise that the damages caused by the Bank's, its responsible person's or employees' severe negligence or intentional violations (Even in this case, relevant compensation is limited to the direct and reasonably expected damages purely and directly arising thereof, if any, or the related transaction amount, whichever is lower.), the Bank shall not be held liable to the Applicant or any other party for the consequences arising from or related to the following:

I. The Applicant's or any other party's (authorized or not) use of the internet banking service or inquiry of any information;

II. The provision of the internet banking service, or the transferring of instructions or information related to the internet banking service, or any interruption, blockage, suspension, delay, loss, inaccessibility, damage or other malfunctioning due to any conduct, negligence or situation beyond the Bank's reasonable control upon connection to websites, including but not limited to any communication network malfunctioning, any third party service provider's conduct or negligence, machinery malfunctioning, electricity outage, function malfunctioning, damage, or equipment, installment or facility insufficiency, or any law, regulation, template, code, instruction, supervisory guidance or governmental orders (legally valid or not), and

III. any transmission of system, equipment or device via any communication network provider, and/or storage of any information and/or data related to the Applicant, the internet banking service and/or the Applicant's transactions or trading via the internet banking service.

IV. Under any circumstance, the Bank or any information provider shall not be held liable for compensation regarding any sudden, indirect, special, derivative or punitive damage, including but not limited to the damages related to the use, income, profit or deposit, or be held liable to the customer or any other party.

V.

Article 27 Record keeping

Both the Bank and the Applicant shall retain all electronic documents that contain trading instructions. Both parties shall also ensure the authenticity, integrity and completeness of the retained records.

The Bank shall perform duty of care in retaining the aforementioned records. The records shall be retained for at least five years.

Article 28 Efficacy of electronic documents

The Bank and the Applicant agree that all electronic documents exchanged according to the terms of the Agreement are equivalent to written instructions.

Article 29 Termination of the Agreement by the Applicant

The Applicant may terminate the Agreement at any time, provided that the termination request is made in person or by methods agreed upon by the Bank.

Article 30 Termination of the Agreement by the Bank

The Bank shall notify the Applicant in writing at least 30 days prior to the termination of the Agreement. However, in any of the following circumstances, the Bank may terminate the Agreement at any time in writing or by any other method agreed upon:

I. The Applicant has assigned rights or obligations of the Agreement to a third party without the Bank's consent.

II. The Applicant is found engage in the following acts: using this service to access data that are not owned by the Applicant, or other misuse of the service, abnormal transactions of substantial amounts or frequency, or destructive or inappropriate behavior involving the use of simulation programs, Trojan horse programs or virus programs.

III. The Applicant is declared bankrupt or undergoes a court-ordered corporate reorganization, or the Applicant files for bankruptcy, liquidation, dissolution or reorganization or does so by a third party.

IV. The Applicant is in breach of the law or other relevant regulations, or the Applicant's accounts have been used (or suspected of being used) for illegal purposes;

V. The Applicant has settled and ceased all deposit and other business dealings with the Bank;

VI. The Applicant has breached provisions of the Agreement and has failed to take corrective action or has failed to fulfill the obligations by the deadline after being notified to do so.

VII. The Bank deems the Applicant's account suspicious of being dummy account for criminal activities, or of any other illegal or improper use, or of illegal or clearly unusual transactions according to the standards stipulated in the "**Regulations Governing the Deposit Accounts and Suspicious or Unusual Transactions"**.

VIII. Pursuant to the "**Guidelines Governing Anti-Money Laundering and Combating the Financing of Terrorism by the Banking Sector**", the account is determined to belong to an individual, legal entity or organization subjected to economic sanctions under the "**Counter-Terrorism Financing Act**"; or to a terrorist or terrorist group identified or investigated by a foreign government or an international anti-money laundering organization. And where the Applicant does not cooperate with the Bank's review, or refuses to provide information on the beneficial owner or the person exercising control over the Applicant, and is unwilling to explain the nature and purpose of transaction, or source of funds;

IX. Other causes deemed reasonable by the Bank to terminate the Agreement with the Applicant.

Article 31 Terms and conditions of the seal

The Applicant agrees that, in order to apply for the internet banking service to the Bank, for all contracts and documents between the Applicant and the Bank related to the internet banking service, including the application for the use and resetting of passwords and the application for and changes of the security control mechanism, shall require the original signature(s) of authorized persons affixed with company seal (if any) for corporate account and the original signature of the account holder for individual account until the Applicant cancels the Bank's internet banking service.

In cases where changes occur to the Applicant's name, organization, articles of organization, seal, representative, representative's access rights or other matters that may affect the Bank's rights, the Applicant shall immediately notify the Bank in writing of the changes, and conduct the change or cancellation of the aforementioned signature(s) of authorized signatories or original signature(s) of authorized persons. For any transactions with or instructions to the Bank prior to the written notice and the completion of the change or cancellation of such signature(s), the Applicant shall bear all responsibilities and compensate the Bank for any damage to the Bank arising thereof.

Article 32 Contract amendments

If any changes are made to the terms of the Agreement, the Bank shall announce such changes either in writing or in a prominent way at the Bank's business premises or on its website instead of notifying the Applicant respectively. The Applicant shall be deemed to have consented to the change(s) if no objection is raised within 7 calendar days thereafter.

Matters not covered herein shall be supplemented or amended in writing through negotiation between the Bank and the Applicant.

Article 33 Delivery of correspondence

The Applicant agrees to use the address or the e-mail address provided to the Bank as the means of delivery for future correspondences. The Applicant is required to notify the Bank in writing or in other methods acceptable to the Bank for any changes to the residential, company or e-mail address. The Applicant also agrees that the Bank deliver future correspondences to the newly updated address or e-mail address after the change has been completed by the Bank. In cases where the Applicant fails to notify the Bank in writing or in other methods acceptable to the Bank for any changes in the address or e-mail address, the changes shall be deemed invalid to the Bank, and the Bank shall use the address or the e-mail address formerly provided to the Bank as the means of delivery for future correspondences.

Article 34 Governing laws and court jurisdiction

This Agreement is governed by and shall be construed in accordance with the laws of Singapore.

The Bank and the Applicant agree to submit all their disputes arising out of or in connection with this Agreement to the exclusive jurisdiction of the Courts of Singapore courts or any other court specified by the Bank.

Article 35 Title

Titles in the Agreement are made to facilitate easy reference and shall not affect the interpretation, description, and understanding of the terms.

Article 36 The Chinese translation thereof is for reference only and the English version shall always prevail in case of any inconsistency between the English version and the Chinese translation thereof.