(2024.03 Version)

Taishin Bank

Personal Internet Banking and Mobile Banking Service Agreement

(Product online membership application)

To protect your rights and interests, please be sure to read the contents of this Agreement carefully. By clicking the "Agree" button, you acknowledge that you have reviewed it within a reasonable period of at least five days, you have fully understood the terms and conditions stated herein, and agreed to abide the contents contained in this Agreement:

Article I Bank information

I. Bank name: Taishin International Bank (hereinafter referred to as the Bank).
II. 24-hour customer service hotline: (02)2655-3355.
III. Complaint handling hotline: (02)2700-3166 and 0800-079-885; Complaints are accepted Monday to Friday, 09:00 - 12:00 and 13:30 - 17:30.
IV. Website: www.taishinbank.com.tw.
V. Bank e-mail: csr@taishinbank.com.tw.
VI. Address: 1F & B1, No. 44, Section 2 Zhongshan North Road, Zhongshan District, Taipei City.
VII. Fax number: (02)5571-9396.

Article II Applicability

I. This Agreement serves as a common agreement for the Bank's **"Internet Banking and Mobile Banking Services"** in general. It applies to all services offered under the Agreement unless specifically arranged otherwise.
II. No other service agreements separately arranged shall contradict the terms of this Agreement. However, special arrangements that offer more protections to members of the Bank's Internet Banking and Mobile Banking Services (hereinafter referred to as Member) may supersede the terms and conditions stated herein.
III. Any ambiguities conveyed by the terms of this Agreement shall be interpreted in the way that reflects the Member's best interest.

Article III Terminology definitions

I. “Internet Banking and Mobile Banking Service”: Refers to the use of computers or mobile devices (e.g., mobile phone, mobile device, personal data assistant (PDA), or any device with a built-in communication module, collectively referred to as "Personal Communication Devices") to access various financial services offered by the Bank over Internet connections, without the Member having to visit a Bank branch office in person (excluding Richart digital deposit services).

II. “Electronic documents”: Refers to any text, audio, image, video, symbol, or other type of data transmitted by the Bank or by the Member over the Internet, which has been arranged in electronic or other form that is not directly recognizable, but can be processed electronically to convey meaning (e.g., text messages, phone calls, emails, etc.).

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

IV. “Certificate”: Electronic data that contains information of how digital signature is to be validated; it is used to verify the signatory's identity and eligibility.

V. “Private key”: Refers to the piece of a paired digital data retained by the signatory; this digital data is used for producing digital signatures.

VI. “Public key”: Refers to the piece of a paired digital data that is issued to the public; this digital data is used to validate digital signatures.

Article IV Website verification

I. Prior to using the Bank’s “Internet Banking and Mobile Banking Service”, please verify the URL of the Bank's Internet Banking Service website or Mobile Banking download and installation software to be correct in order to ensure easy access to Internet Banking Services or successful component download or installation of the Mobile Banking app. Please contact the Bank’s customer service if you have any questions.

II. The Bank shall on a non-periodic basis convey the risks involved in using the Internet Banking and Mobile Banking environment through email or announcements on the Bank’s official website in manners that are understandable to the average person.

III. The Bank shall exercise its due care of a good administrator to maintain the correctness and security of website information. The Bank shall also be on the lookout for webpage forgeries to prevent losses to the Member.

Article V Services

If the following services are determined by the competent authority or the Bank to be service items that need to be added or removed, they shall be handled in

accordance with Article 23 of this Agreement, and shall be announced at the Bank's business premises or on its official website.

Online membership application for credit card products:

I. **The Applicant completes the membership application process of the Bank's credit card Internet Banking and Mobile Banking with the information of any primary or supplementary cardholder of the Bank (including but not limited to any credit card information and various personal information of the original application for the credit card).**

II. Credit card product online membership application services include:

1. Credit card balance inquiry service
2. Credit card e-Statement service (limited only to primary cardholders)
3. Credit card points inquiry (limited only to primary card holders)
4. Credit card cash advance service
5. Personalized services

III. If you apply for membership online for credit card products and then visit a branch of the Bank to open a NTD account and apply for full-featured Internet Banking and Mobile Banking transaction membership, your online membership application for our Internet Banking and Mobile Banking products will change to a transactional membership.

Online membership application for banking products:

I. **The Applicant completes the application process for the Bank's Internet Banking and Mobile Banking transaction membership with the Bank's designated NTD account and the One Time Password (OTP) sent to the personal mobile communication device associated with the mobile phone number and email stated in the Applicant's information on file at the Bank.**

II. Online membership application services for banking products include:

1. NTD/foreign currency services.
2. Loan services.
3. Fund/securities/trust-related services.
4. Credit card services.
5. Personalized services.

III. **Token authentication**

1. To conduct NTD fund transfers to non-designated accounts over the Bank's

Internet/Mobile Banking system, the Applicant must have full-featured Internet/Mobile Banking transaction membership. The Applicant may then choose to receive the initial password in one of the following ways to self-authenticate the token used:

(I) Visit a Bank branch office in person and follow the directions of the teller, then set an initial password by entering the password into the PIN pad, and authenticate the token before the next day; the initial password shall be voided after the expiry described above.

(II) Collect a password slip from the Bank in person, have the Bank proceed with application procedures, and authenticate the token using a personal communication device within 30 days after application; the initial password shall be voided after the expiry described above.

(III) Insert a valid IC ATM Card issued by the Bank into a compatible card reader, log in to the Bank's Internet/Mobile Banking system, and follow the instructions to authenticate the token used.

(IV) The Applicant is required to insert a valid IC ATM Card issued by the Bank into the Bank's Internet/Mobile Banking Service System, and follow the instructions to authenticate the token used.

(V) The applicant receives the activation password by text message on the mobile phone, and then completes device authentication according to the instructions.

2. The Applicant may conduct transactions such as transfers to non-designated accounts, bill payments, and card-free withdrawals through select mobile devices, such as cell phones and iPads (compatible devices shall be as listed by the Bank's official website). The Applicant must authenticate the device with the initial password acquired under the preceding paragraph before conducting the aforementioned transactions through the device.

Article VI Internet connection

I. The Bank and the Member both agree to transmit and receive electronic documents over the Internet. The Member has the responsibility to ensure the

accuracy and validity of information maintained on the Bank's Internet Banking and Mobile Banking Systems. The Bank shall be indemnified from any losses and inconvenience caused by the Member’s failure to update personal information, which result in the absence or inefficiency of messages delivered.

II. The Bank and the Member shall establish 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 VII Receiving and responding to electronic documents

I. Upon receiving digital signatures or any electronic document agreed upon by the Bank and the Member as proper means of identification, the Bank shall prompt for the Member's confirmation by displaying key information on the webpage (except for inquiries) before proceeding with the verification and execution. The results of the verification and execution shall be notified to the Member in writing, via electronic document (including email and APP push notification) or in the method agreed between the two parties.

II. In circumstances where the Bank or the Member is unable to determine the identity or the contents of electronic document sent by the other party, the electronic document shall be considered as never having been sent in the first place. However, where it is possible for the Bank to ascertain the Member's identity, the Bank shall notify the Member of the fact that the message contents were unidentifiable in writing, via electronic document (including email and APP push notification) or using methods agreed upon by the two parties.

Article VIII 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. When the Bank is unable to debit from the Member's account for the amount payable, for reasons that are attributable to the Member.

Where the Bank does not executes the electronic documents in the preceding paragraph, it shall simultaneously notify the Member of the reasons and circumstances of the non-execution in writing, via electronic document (including email and APP push notification), or using methods agreed upon by the two parties.

Members can confirm with the Bank by phone after receiving the notification. However, the Bank is not responsible whatsoever for non-executions that are due to bad signal qualities over the course of transmission.

Article IX Timeframe for electronic document exchanges

I. All electronic documents are automatically processed by the Bank's computer. The Member cannot recall an electronic document once it has been confirmed by the Member according to the method described in Article 7, Paragraph 1. However, the Member can recall or amend scheduled transactions that are yet to fall due, subject to the timeframe specified by the Bank.

II. If the electronic document reaches the Bank's system through the Internet after service hours (detailed business hours are prompted on the webpage or announced at the Bank's website), the Bank shall notify the Member via electronic document that the transaction shall be postponed to the following business day or handled using other agreed methods.

Article X Costs

I. The Member shall pay service fees, handling charges, postage and cable charges according to the standard rates stipulated by the Bank on the webpage below (https://www.taishinbank.com.tw/TSB/personal/common/legal-disclaimers/TSBankPublicDisclosure-000006/), and authorize the Bank to collect all fees and charges from the Member's deposit account. The Bank may not collect any charges it has not advised in the first place.

II. Any subsequent change to the standard rates mentioned above must be published on the Bank's website in a clear, visible manner, and notified to the Member using methods agreed upon by the two parties (referred to as "Notice" below).

III. If the adjustment described in Paragraph 2 results in a higher rate, the Bank shall provide the Member with the option to agree or disagree with the higher rate over its webpage. If the Member does not agree before the effective date of adjustment, the Bank may suspend part or all Internet/Mobile Banking services offered to the Member on the date the adjustment takes effect. If the Member agrees to the rate adjustment after the effective date, the Bank shall immediately restore the Member's access to all relevant Internet/Mobile Banking services in accordance with the Agreement.

IV. The Bank shall issue the abovementioned announcements and Notices at least 60 days prior to taking effect, and the effective date of adjustment cannot be set earlier than the beginning of the year following the announcement/Notice.

Article XI Member Software/Hardware Installation and Associated Risks

I. The Member shall self-install computer software, hardware, and any security-related equipment or software (such as anti-virus software) on his/her computer or personal communication devices required for using the services under the terms and conditions. **The Member shall also bear all costs and risks associated with the installation.**

II. Where the software, hardware and documents in Paragraph 1 are provided by the Bank, the Bank agrees only to use by the Member within the scope of the services, and such software, hardware and documents shall not be transferred, loaned, or in any other way given to a third party. The Bank shall also describe on its website and on the packaging of software/hardware provided the minimum system required to run the service, and risks associated with the software/hardware supplied.

III. The Bank may request that the Member return the supplied equipment mentioned above upon termination of the Agreement, but only if it has been separately arranged under the Agreement.

Article XII Member's Connection and Responsibility

I. Where special arrangements exist between the Bank and the Member, connection may commence only after the necessary tests are completed.

II. **The Member is responsible for safekeeping any User ID, PIN, certificate and other identification tools agreed with the Bank, and shall not provide the above to a third party for use or safekeeping to ensure transaction security.**

III. When applying for Internet Banking and Mobile Banking services, the Member is required to set one "User ID" and one "PIN" to be used for identification; the PIN must be a combination of English alphabets and numeric characters; there is no limit to the amount of times a PIN may be changed.

IV. If the Member makes incorrect PIN entries after four consecutive attempts, the Bank's system shall automatically suspend the Member from accessing services offered under the Agreement. To resume use of service, the Member must submit an application in the manner required by the Bank.

V. Both the Internet Banking System and the Mobile Banking System accept the same "User ID" and "PIN". If there are two or more users attempting to log in simultaneously to the Bank's Internet/Mobile Banking system using the same ID number, the Bank shall deny all login attempts made after the first user.

Article XIII Transaction Verification

I. For every instruction processed, the Bank shall notify the Member of the outcome in writing, via electronic document (including email and APP push notification) or other methods agreed by the two parties, and the Member should verify whether the outcome contains any errors. Any inconsistencies

must he reported to the Bank in writing, via electronic document, or using methods agreed upon by the two parties within 45 days after the transaction is completed; the Bank shall then conduct the necessary investigations.

II. The Bank shall compile a statement of transactions conducted in the previous month, and deliver to the Member on a monthly basis in writing, via electronic document (including email and APP push notification), or using methods agreed upon by the two parties (no statements shall be delivered for months where no transactions took place). The Member should verify all items listed in the transaction statement, and report any errors found in writing, via electronic document, or using methods agreed upon by the two parties within 45 days after receiving the statement for the Bank to conduct investigations.

III. The Bank shall conduct immediate investigation upon receiving the Member's error report, and inform the Member the outcome of the investigation in writing, via electronic document (including email and APP push notification), or using any method agreed upon by the two parties within 30 days after receiving the Member's report.

Article XIV Responding to errors in electronic documents

I. In the event that the Member encounters any errors in the electronic document for reasons that are not attributable to the Member, the Bank shall assist the Member in rectifying the error and offer other assistance as deemed necessary.

II. If the above errors are attributable to the Bank's mistakes, the Bank shall rectify immediately upon being informed, and notify the Member of such errors in writing, via electronic document (including email and APP push notification) or other methods agreed by both parties.

III. In the event that the Member transfers funds into the wrong account or at the wrong amount by mistakes such as inputting an incorrect Bank ID, account number, or amount using services stated herein, the Bank shall provide the following assistance immediately upon being notified by the Member:

1. Provide details relating to the transaction to the extent permissible by law.
2. Notify the receiving bank for assistance.
3. Report the results.

Article XV Authorization and Responsibilities Associated with Electronic Documents

The Bank and the Member shall ensure that all electronic documents transmitted to the other party are legally authorized. Should the Bank or the Member discover any misuse or theft of User ID, PIN, certificate, private key, or any unauthorized conducts by a third party, the Bank and/or Member shall immediately notify the other party in writing, via electronic document (including email and APP push notification) or using

methods agreed by both parties to suspend the use of service and take the necessary precautions.

The Bank shall be responsible for the outcome of the third party's use of service before the notice is received. This excludes any one of the following circumstances:

I. The Bank is able to prove that the misuse is due to the Member’s intentional or negligent acts.
II. The misuse happens more than 45 days after the Bank transmits transaction data or an account statement in writing, via electronic document (including email and APP push notification) or other methods agreed by both parties. However, special circumstances (e.g. long-distance travel, hospitalization, etc.) where the Member is unable to notify the Bank at the time of occurrence are excluded; in such a case, the 45-day period shall begin from the day the special circumstance ends, unless the delay is attributable to an intentional or negligent act on the part of the Bank.

The Bank shall bear the costs of investigation into the misuse and theft described in Paragraph 2.

Article XVI IT System Security

I. The Bank and the Member must ensure the security of their own systems, and take proper measures to protect records and personal information from intrusion, illegal access, theft, alteration, or destruction.
II. Where there is a dispute over whether the Bank's protective measures have been breached or its security weaknesses have been exploited by a third party, the Bank is responsible for providing evidence proving that such incidents did not occur.
III. The Bank is liable for compensation of the Member for any damages ensuing from third-party intrusion into its information systems.
IV. If the Member forgets to log off from the Bank's Internet/Mobile Banking System, or if the system detects 5 minutes of inactivity (or, if the Member otherwise sets a duration of no more than 10 minutes before log-off, the time agreed by the Member and the Bank shall prevail), the Bank shall automatically log off the Member from the Internet/Mobile Banking System.

Article XVII Obligation of Confidentiality

I. Unless otherwise regulated by law, the Bank must ensure that electronic documents exchanged with the Member and any information obtained while 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 Member has given consent to disclose such information to a third party, the third party must be made to comply with this confidentiality clause.

II. A third party's failure to comply with the confidentiality requirements is considered a violation of the Bank's obligation to inform.

Article XVIII Damage Compensation

The Bank and the Member agree that any delays, omissions, or errors in transmitting or receiving electronic documents in accordance with the Agreement, which give rise to the losses of the other party, shall be compensated by the party whom the cause is attributable to.

Article XIX Record Retention

Both the Bank and the Member shall retain all electronic documents that contain trade instructions. Both parties shall also ensure the authenticity and integrity of retained records. The Bank shall exercise its due care of a good administrator in maintaining the aforementioned records. The records shall be retained for at least 5 years, or for whatever longer durations stipulated by law.

Article XX Efficacy of Electronic Documents

The Bank and the Member agree to use electronic documents as means of exchanging instructions. All electronic documents exchanged according to the terms of the Agreement are equivalent to instructions issued in writing. This excludes circumstances where the laws have regulated otherwise.

Article XXI Membership Termination Agreement

The Member may terminate this Agreement at any time, provided that the termination request is made in person, in writing, via electronic document, or using any methods agreed by both parties.

Article XXII The Bank's Termination or Suspension of the Agreement

The Bank shall notify the Member in writing, via electronic document (including email and APP push notification), or using any method agreed by both parties at least 30 days in advance when terminating this Agreement. **However, in any of the following circumstances, the Bank may terminate this Agreement by notifying the Member at any time in writing, via electronic document (including email and APP push notification) or using any method agreed by both parties:**

I. **The Member has assigned the rights or obligations of this Agreement to a third party without the Bank's consent.**
II. **The Member declares bankruptcy according to the Bankruptcy Act, or undergoes debt rehabilitation or liquidation according to The Consumer Debt Clearance Statute.**
III. **The Member has violated Articles 15 to 17 of this Agreement.**
IV. **The Member is in violation of other terms of the Agreement, and has failed to rectify or fulfill obligations within the timeframe specified by the Bank.**

In any one of the circumstances described below, the Bank may suspend the Member's login access to the Internet/Mobile Banking Service System or to other electronic payment services without prior notice for security concerns:

I. The account is suspected to have been misused or used for inappropriate purposes (including but not limited to using the Bank's Internet/Mobile Banking for arbitrage transactions), either being informed by a government institution or that the Bank has established reasonable judgments based on material facts.
II. The Member has not logged in to the Bank's Internet Banking or Mobile Banking System for 12 consecutive months.

Article XXIII Amendment of the Agreement

If any changes are made to the terms of the Agreement, the Bank shall notify the Member of such changes in writing, via electronic document (including email and APP push notification), or using methods agreed by both parties, and through a public announcement at the Bank's place of business or on its website. The Member shall be regarded as having consented to the change(s) if no objection is raised within 7 days thereafter. For the following changes, however, the Bank shall notify the Member in writing, via electronic document (including email and APP push notification) or using methods agreed by both parties at least 60 days prior to the effective date as well as at the Bank's place of business and on its official website. The notification must include detailed descriptions of the changes and comparisons of the original and revised terms in a clear manner, informing the Member of its right to object before the changes take effect. If no objection is raised by the Member before the effective date, the changes are considered accepted by the Member. The Member also needs to be informed that the Bank shall terminate the Agreement if the Member chooses to object during the given period:

I. Changes in methods of notifying the other party for theft or misuse of User ID, PIN, certificate, private key, or any unauthorized conducts.
II. Other matters stipulated by the competent authority.

Article XXIV Report of Loss

With regard to losses reported over the Bank's Internet/Mobile Banking System (including the loss of an ATM Card, account passbook, certificate of deposit, authorized seal, etc., but excluding the loss of a check), the loss of an ATM Card shall be deemed to have been duly reported after the reporting procedure has been completed through the Internet/Mobile Banking System; thereafter, the Member shall not need to issue a written report at the branch; for reports of losses other than ATM Card, the Bank simply stops further payments against such media, and the Member still needs to visit a Bank office during business hours to report the loss in writing.

Article XXV Delivery of Correspondence

The Member agrees that the address indicated in the Agreement shall be the location to which the relevant documents are sent. In the event of a change of address, the Member shall inform the Bank in writing or via another method agreed upon and agrees that the changed address shall be the location to which the relevant documents are sent. If the Member has not changed its address in writing or via a method agreed upon, the Bank shall send all the relevant documents to the address indicated in the Agreement or to the address the Member most recently provided.

Article XXVI Applicable Laws

The Agreement shall be governed by the laws of the Republic of China.

Article XXVII Jurisdiction

In the event of litigation, the Bank and the Member agree Taiwan Taipei District Court shall be the court of first instance. However, this does not supersede Article 47 of the Consumer Protection Act or Article 436-9 of the Code of Civil Procedure, where litigations involving small sums may be subjected to different jurisdictions.

Article XXVIII Headings

The various titles of the Agreement have been presented for ease of reference, and do not affect the interpretation, description, and comprehension of the clauses under the Agreement.

Article XXIX Agreement

The Agreement is executed in duplicate, with the Bank and the Member each retaining one copy. The content of the Agreement can be copied by the Applicant when applying for Internet Banking and Mobile Banking services of the Bank, or the content of the latest agreement can be downloaded from the website of the Bank at any time.