[NOTE: This is an English translation of Japanese original. The governing language of this agreement shall be Japanese. Only the Japanese original shall have the effect of a contract and the English translation herein made for reference shall have no effect.]

SHINSEI BANK

Shinsei Corporate Direct Transaction Agreement
As of January 4, 2019

This agreement describes how Shinsei Bank (hereinafter referred to as the "Bank") conducts business when corporate customers (hereinafter referred to as the "Users") transact from Shinsei Corporate Direct, the internet banking service.

Shinsei Corporate Direct is, as a general rule, an exclusive service for corporate customers located inside Japan.

1. Services offered by Shinsei Corporate Direct

Shinsei Corporate Direct shall be available when the following services and transactions (hereinafter referred to as the "Services") are requested by the operator who is granted by the User an authority to use Shinsei Corporate Direct, by means of computer terminals in accordance with the Bank's guidelines. Available Services are:

(1) Account Inquiries
Various inquiries including balance inquiries and account activity inquiries of the deposit account which the User registered with the Bank in advance (hereinafter referred to as the "Account in Use").

(2) Fund Transfers (The following provisions do not apply to users of the "account inquiries only" (*koza-shoukai-senyo*) service.)

(a) Transfers within the Bank
To withdraw money from the liquid deposit of the Account in Use (e.g., yen ordinary account, yen current account) and then to credit it to the liquid deposit of the same or another Account in Use, or other deposit account(s) held by customers in the Bank.

(b) Bank Transfers
To withdraw money from the liquid deposit of the Account in Use and then to send a notice of credit to an account held in a financial institution other than the Bank that is located inside Japan.

2. Application for Use

To apply for the Services, an applicant is requested to submit the application form prescribed by the Bank upon approval of this Agreement. If prerequisites prescribed by the Bank are unfulfilled, the Bank may decline to provide the Service.

3. Computer terminals for use

The type of computer terminals for use of the Services is limited to computers prescribed by the Bank.

4. Service Hours

The Services are available within the hours predetermined by the Bank, which may differ depending on the service or transaction. However, in an unavoidable event such as system maintenance or system failure, the Bank may alter the service hours without prior notice to the Users.

5. Corporate Administrator

(1) For the application of the Services, a Corporate Administrator's name and contact shall be identified.

(2) The Corporate Administrator shall be responsible for controlling the following matters:

(a) Neither Corporate ID nor Administrator's ID, which were registered when the application was made, are disclosed or leaked to the person(s) unauthorized by the User (hereinafter referred to as the "Information Control");

(b) Setting, changes, and Information Control of the Administrator's password for the use of the Service;

(c) Registration, revision, and deletion of the computer terminal operator (hereinafter referred to as the "Operator") in order to use the service;

(d) Information Control of the Operator's ID that is created at the time of registration set forth in the preceding item;

(e) Setting and revision of the Services available for each Operator and the Account(s) in Use.

(f) Appointment of an appropriate Operator and establishment of the appropriate limit of the transaction amount in order to promote the appropriate and safe use of the Services;

(g) Entry of registration for the use of a one-time password token when logging into the computer by the Administrator's ID (This applies only when the one-time password method is adopted); and

(h) Other matters prescribed by the Bank.

(3) The Bank assigns and notifies a temporary Administrator's password to the Corporate Administrator who is reported to the Bank as set forth in Paragraph (1) above. The Corporate Administrator shall change this temporary Administrator's password to an Administrator's password at the initial use of the Services.

(4) When the Corporate Administrator changes the Administrator's password, the Corporate Administrator him/herself shall handle such a change by using the Helpdesk function.

(5) When the Corporate Administrator cannot remember the Administrator's password, he/she shall follow the change procedures prescribed by the Bank.

6. Helpdesk Function

The Helpdesk function is used in the Services by the Corporate Administrator for the control set forth in the Paragraph (2) of the preceding Article within his/her own responsibility. The use of the function is limited to the Corporate Administrator.

7. Passwords

(1) Corporate Administrator

The Corporate Administrator may initiate the Services by entering the Corporate ID registered for each User, the Administrator's ID of the Corporate Administrator, and the Administrator's password set by the Corporate Administrator by changing the temporary password and logging into the computer terminal based on an authentication method set forth in Paragraph (1) of Article 8 (However, the one-time password method set forth in Paragraph (1)-(c) of Article 8 is available only when it is adopted),

(2) Operator

The Operator may initiate the Services by entering the Corporate ID registered for each User, the Operator's ID registered for each Operator, and the Operator's password set by each Operator by changing the password initially registered by the Corporate Administrator for each Operator and logging into the computer terminal based on an authentication method set forth in Paragraph (1)-(a) and -(b) of Article 8. If the Operator is granted by the Corporate Administrator the authority for approving a transaction, he/she may approve the transaction by entering a one-time password (only when the one-time password method is adopted.)

8. Authentication Method (Login Method and Transaction Approval Method)

(1) The three authentication methods (i.e., login and transaction approval methods) provided to use the Services are: i) the "electronic authentication method" and ii) "fixed password authentication method for the Corporate Administrator and the Operator to log into the computer terminal, and iii) the "one-time password method" that is used to log into the computer terminal by the Administrator's ID or to approve a bank transfer/fund transfer transaction by the Operator's ID.

(a) Electronic authentication method (Login method)

This uses the Corporate ID, Operator's ID (or Administrator's ID in the case of the Corporate Administrator), Operator's password (or Administrator's password in the case of the Corporate Administrator), and electronic certificate to identify the User.

(b) Fixed password authentication method (Login method)

This uses the Corporate ID, Operator's ID (or Administrator's ID in the case of the Corporate Administrator), and the Operator's password (or Administrator's password in the case of the Corporate Administrator) to identify the User.

(c) One-time password method (Login method and transaction approval method)

(This method is applicable when a "fund transfer transaction" service is used, but is not applicable to "account inquiries only" users.)

The authentication methods (a) and (b) above are available for logging into the computer terminal. In addition to these methods, this one-time password method is used to identify the User through the entry of a one-time password made at the time of login by the Administrator's ID, and at the time of the approval by the Operater's ID of a bank transfer/fund transfer transaction.

*One-time passwords are automatically updated after the elapse of a certain period of time. They will be invalidated once used to log into the computer terminal by the Administrator ID or used by the Operator's ID to approve a bank transfer/fund transfer transaction.

(2) The electronic authentication method shall be, in principle, applied to use the "account inquiries only" service, while the combination of the electronic authentication method and the one-time password method shall be applied when a fund transfer transaction service is used. However, if there is a compelling reason such as the environment of a computer terminal, the fixed password authentication method may be allowed in order to use the "account inquiries only" service. Further, the electronic authentication method (i.e., not combined with the one-time password method) or a combination of the fixed password authentication method and the one-time password method may be allowed for the fund transfers service.

(3) Change of the authentication method: It is allowed to i) change from the fixed password authentication method to the electronic authentication method and ii) add the one-time password method to the electronic authentication method or the fixed password authentication method in order to conduct fund transfer transactions. However, it is not allowed to change the

method from the electronic authentication method to the fixed password authentication method or cancel the one-time password method.

(4) Electronic certificate

(a) If the User changes the authentication method to the electronic authentication method, the User shall install an electronic certificate issued by the Bank in the computer terminal using the method prescribed by the Bank. The Corporate ID registered for each User, Operator's ID (or Administrator's ID in the case of the Corporate Administrator) and the Operator's password (or Administrator's password in the case of the Corporate Administrator) are required for this installation.

(b) An electronic certificate shall be only valid during the period prescribed by the Bank (hereinafter referred to as the "Validity"). The User shall renew the electronic certificate by the method prescribed by the Bank before expiration of the Validity. If the User cancels the Services, the installed electronic certificate will be forfeited.

(c) When the User transfers, discards, or disposes of a computer terminal with an electronic certificate installed, the User shall go through the procedures to forfeiting the electronic certificate beforehand by the method prescribed by the Bank. If the User fails to go through such procedures, the Bank will not be responsible for any damage attributable to the unauthorized use of the electronic certificate or to other incidents if such an incident occurs.

(5) One-time password

(a) Users are requested to use the method prescribed by the Bank and download the relevant application software in order to obtain a software token.

(b) If an erroneous one-time password is successively entered more than the number of times prescribed by the Bank, the one-time password authentication method shall be suspended. If such erroneous operation occurs, the Bank shall not assume any responsibility for any damage caused by such suspension. If the User wishes to resume the one-time password authentication method, he/she is requested to take the procedures prescribed by the Bank.

9. Identity Verification

(1) When the Bank confirms that the Corporate ID, Operator's ID (or Administrator's ID in the case of the Corporate Administrator), the Operator's password (or Administrator's password in the case of the Corporate Administrator), the electronic certificate (in the case of the electronic authentication method), and the one-time password (in the case of the one-time password method) (hereinafter, collectively referred to as the "authentication data"), all of which are received in relation to the Services, match the authentication data registered at the Bank, the Bank decides that the relevant computer operation has been conducted by the Corporate Administrator/Operator to whom an appropriate authority is granted by the User and makes the Service available.

(2) If the Bank confirms that the received authentication data match the authentication data registered at the Bank and then renders the Services as set forth in the preceding paragraph, the Bank will not be responsible for any damage attributable to the counterfeiting, falsification, plagiarism, unauthorized use and other incidents of these authentication data if such an accident occurs.

(3) The authentication data are requested to be strictly controlled so that they will not be disclosed to any parties except the Corporate Administrator and the Operator. The Bank is not responsible for controlling the authentication data. If the Operator's password or the Administrator's password is suspected to be stolen or leaked, it is advised to immediately change the password at the Services screen (Helpdesk screen, in the case of the Corporate Administrator). If the electronic certificate is suspected to be stolen or leaked, it is advised to contact the Call Center connected by the telephone number of the "Corporate Call Center" described by the Bank and make request for the procedures to forfeit the electronic certificate and reissuing an electronic certificate.

(4) If the Operator's password is wrongly entered beyond the number of times prescribed by the Bank, the Services will be suspended. In order to resume the use of the Services, the Operator shall contact the Corporate Administrator, and the Corporate Administrator shall unlock the suspension of the Services at the Helpdesk screen. When the Corporate Administrator wrongly entered Administrator's ID and Administrator's password beyond the number of times prescribed by the Bank, the Services will be suspended as well. In such a case, in order to resume the use of the Services, the Corporate Administrator shall contact a telephone center that can be connected through the telephone number designated by the Bank under the name of the "Corporate Call Center" and make a request to unlock the suspension of the Services.

(5) If the Operator cannot remember the Operator's ID or the Operator's password, he/she contacts the Corporate Administrator. The Corporate Administrator resets the password using the function on the Helpdesk screen as prescribed.

(6) If the Corporate Administrator cannot remember the Administrator's password, he/she contacts the Corporate Call Center and asks for the password to be reissued. In such an event, in accordance with the procedures prescribed by the Bank, the Bank will reissue and send a temporary password decided by the Bank to the Corporate Administrator by mail. When logging on with the temporary password for the first time, it is necessary to change this password to any Administrator's password.

10. Request, Reception, Conclusion of the Fund Transfer Transactions (The following provisions do not apply to "account inquiries only" (*koza-shoukai-senyo*) users.)

(1) How to request the fund transfers

In order to request a fund transfer transaction through the Services, after logging into the computer terminal by the Corporate Administrator, the Operator who is granted the authority by the Corporate Administrator operates the computer terminal, goes through the identity verification process set forth in the preceding Article, and enters the transaction details accurately pursuant to the method prescribed by the Bank. After that, the Operator, who is granted by Corporate Administrator an authority to approve the transaction, also goes through the identity verification process (including one-time password authentication for transaction approval) set forth in the preceding Article, and then approves the details of the transaction. The request is made when all the information entered is transmitted to the Bank.

(2) Confirmation of the Request Details

(a) The request is deemed to have been confirmed when the request details have been received by the Bank pursuant to the preceding Paragraph.

(b) For the fund transfers on the day of the request, withdrawal and deposit is executed on the day the request was transmitted to the Bank pursuant to the preceding Paragraph.

(c) For the future dated fund transfers, withdrawal and deposit is executed at the time of the change to the date designated by the request set forth in the preceding Paragraph.

(d) As for the bank transfer on the day of the request, the transaction is executed on the day of the request only when the request details set forth in the preceding Paragraph is transmitted to the Bank before the closing time for the same-day execution prescribed by the Bank. When the request details mentioned in the preceding Paragraph is transmitted after the closing time for the same day execution prescribed by the Bank, a notice of the transaction is sent out as of the next business day (limited to the day when Zengin domestic remittance system is in operation). In that case, funds withdrawn on the day of the request received as set forth in the preceding Paragraph are not subject to any interest.

(e) For the future dated bank transfers, the transaction is processed at the beginning of the business hours for the same-day execution prescribed by the Bank on the day designated by the request set forth in the preceding Paragraph.

(f) For the transaction on the day of the request, the request cannot be cancelled or changed once the transaction details are confirmed. However, a request may be cancelled if it is for future dated transaction and the Bank has not yet processed the transaction. The Services does not accept a reverse transaction.

(3) Withdrawals of Funds and Charges for Fund Transfers

(a) In fund transfer transactions, the Bank may withdraw the funds and charges for the fund transfers automatically from the Account in Use without the User's submitting the withdrawal request or any form of cards.

(b) Funds and charges for the fund transfers set forth in the preceding item may be withdrawn on the day the request is made even when the fund transfer is set to be executed on the following business day.

(4) Refund

In bank transfer transactions, if funds cannot be credited to a recipient's account and are returned by the destination bank, the Bank will credit the funds back into the Account in Use from which the funds were withdrawn, without receiving a request for reverse transaction from the User. The Bank will not be responsible for the loss caused by this transaction to the User. Further, the Bank will not refund the charges for the fund transfer or any other charges.

11. Request, Receipt and Conclusion of the Inquiry Services

(1) How to request the inquiry service

To request the inquiry service through the Services, the Operator who is granted an authority by the Corporate Administrator enters the request at the computer terminal, goes though the identity verification process as set forth in Article Nine (9), and enters the request details accurately pursuant to the method prescribed by the Bank. The request is made when the information entered is transmitted to the Bank.

(2) Confirmation of Request Details

In the inquiry service, the details of the request shall be deemed to have been confirmed when they had been transmitted to the Bank pursuant to the preceding Paragraph, thereby the Bank provides replies and guidance in accordance with its prescribed method.

12. Waivers

(1) The Bank is responsible only for the User's request received by the Bank through the computer terminal. Further, the Bank is not responsible for any damage caused outside the service hours and any damage caused by the following reasons, provided that compensation prescribed by the Bank for fraudulent withdrawals from deposits and so forth in the Internet banking for corporate customers shall follow the procedures concerning such compensation:

(a) If the Services are delayed or failed by disasters, incidents, other causes beyond control of the Bank such as certain actions taken by public authorities like court of law, or by the matters that are not liable to the Bank;

(b) If the Services are delayed or failed due to the trouble in the communication means including failure of the communication equipment or lines and interruption of telephone services or if the Bank transmits incomplete or insufficient information;

(c) If the Contractor's passwords and other transaction information are leaked by tapped telephone and other communication lines;

(d) If the Services are delayed or failed due to reasons caused by the Internet providers, failures of browsing software or the delay/failures of one-time passwords caused by the one-time passwords provider, or the Bank transmits incomplete or insufficient information;
(e) If a system failure is caused by a computer virus; or
(f) If the damage is caused to the User's computer terminal, or the information and/or the software received by the User due to the reasons that are not attributable to the Bank, such as a willful or negligent misconduct by the Corporate Administrator and/or the Operator.

(2) If the User conducts any transaction related to the transactions based on the Agreement from outside Japan due to the User's failure to notify the change of his/her address or for any other reasons, such a conduct is deemed to have been performed inside Japan, and therefore only Japanese laws shall be the governing laws. The Bank accepts no responsibility for the damages caused by the User conducting Agreement-based transactions outside Japan.

13. Cancellation

(1) If all the Accounts in Use are cancelled, the Services for the User are deemed to have been also cancelled. In the event of the partial cancellation of the Accounts in Use, the Services will remain provided in relation to the Account(s) in Use other than the cancelled as long as such Account(s) remain.
(2) If the Service was not used for a period of time prescribed by the Bank or longer, the Bank may possibly suspend all or part of the Services.
(3) If any one of the events set forth in the items below occurs with respect to the User, the Bank may at any time suspend all or part of the Services without any notice from the Bank.
(a) If any payment by the User is suspended, or if a petition for commencement of any domestic or overseas bankruptcy procedure including bankruptcy procedures, civil rehabilitation procedures, corporate reorganization procedures, or special liquidation) is filed;
(b) If the transactions of the User is suspended by a clearinghouse;
(c) If any order or notice of provisional attachment, preservative attachment, or attachment is sent out with respect to the deposit receivables or other receivables held by the User against the Bank;
(d) If the User's whereabouts become unknown to the Bank due to the User's failure to notify the Bank of change of his/her address or any other causes; or
(e) If a reasonable and probable cause, such as providing alternative services or suspension of a part of the Bank's businesses including the Service, necessitates the Bank to suspend all or part of the Services.

14. Changes in Reported Matters

(1) Any change to the items reported for application for the Services (e.g., the User's name, representative, registered seal, address, and Corporate Administrator) must be promptly notified to the Bank in writing using the form designated by the Bank. The Bank is not liable for any losses or damages caused or detected before the notification.
(2) If any notice given by the Bank or any documents dispatched by the Bank are delayed or fail to reach the User because of the User's failure to notify the Bank of changes to the reported items as set forth in the preceding Paragraph, the notice or documents shall be deemed to have arrived at the time they normally should have arrived.

15. Placement of a Seal for Application, Revision, and Cancellation

In transactions in which the Bank has deemed the User's seal impression genuine after checking with reasonable care the seal impression on filed documents or any other documents against the User's seal impression filed with the Bank, the Bank is not liable for any losses or damages arising from forgery or alteration of the documents or any other incidents with respect to the documents.

16. Prohibition on Assignments

The User may not assign, establish pledges or any other rights of a third party on, or make a third party use, its rights related to the Services.

17. Governing Law and Jurisdiction

Japanese laws, regulations and rules shall govern the Services. When a lawsuit becomes necessary with respect to the Services, either the Tokyo District Court or the district court having the jurisdiction in the locale in which the branch having the actual transaction with the User is situated has jurisdiction over it.

18. Application *mutatis mutandis* of the Agreement

Among the matters not provided for in this Agreement, the handling of the Accounts in Use shall be treated in accordance with the related deposit agreements.

19. Revision to the Agreement

The Bank may, at its discretion, revise the Agreement without a prior notice to the Users. After the day of such a change, the Bank

shall handle the Services in accordance with the revised Agreement. When the Agreement is revised, as a general rule, the details of the revision are posted at the counters of the Bank's Head Office and branches as well as on the Bank's Internet website.

End

[NOTE: This is an English translation of Japanese original. The governing language of this agreement shall be Japanese. Only the Japanese original shall have the effect of a contract and the English translation herein made for reference shall have no effect.]

登録 No.7928-E 19.01