GENERAL TERMS AND CONDITIONS OF e-BANKING SERVICES
PT BANK OCBC NISP TBK

1. GENERAL

A. Definition

If it is not explicitly stated otherwise in the Terms and Conditions of Account Opening and Arrangement of PT Bank OCBC NISP, Tbk, the terms below shall have the following meanings:

1. "**Transaction Data**" is data of financial transactions of a Customer's account at the Bank for the last 1 (one) month period and so on provided that the Customer will not receive a current account transaction if there is no transaction in the reporting period.
2. "**E-Banking Services**" are banking facilities owned by the Bank that can be accessed through electronic means which includes:
   a. Automatic Teller Machine (ATM);
   b. Internet Banking;
   c. e-Statement;
   d. ONe Wallet;
   e. Call OCBC NISP;
   f. Autopayment OCBC NISP;
   g. Automatic Fund Transfer;
   h. SMS OCBC NISP;
   i. ONe Mobile;
3. "**Bank Facility Form**" is a form that contains e-Banking Services and its attachments and/or amendments and/or additions from time to time.
4. "**Holidays**" are Saturdays and Sundays and other national holidays determined by the government of the Republic of Indonesia and the days on which the Bank does not operate as determined by Bank Indonesia.
5. "**IVR (Interactive Voice Response)**" is one of the OCBC NISP Call services that can be accessed by the Customer via telephone/ mobile phone to conduct Financial Transactions and Financial Information.
6. "**Financial Information**" is information that includes information on balances and account mutation information.
7. "**Internet Banking**" is a facility provided to Customers for conducting banking transactions through the internet.
8. "**Call Center Card**" is a facility for business entity Customers to access Call OCBC NISP service.
9. "**Response Code**" is a code issued by a Token, either an SMS Token or an Internet Banking Token.
10. "**E-Statement Service**" is a banking service provided by the Bank to the Customer which includes sending Transaction Data reports through e-mail sent by the Bank to the Customer's e-mail address registered in the Bank system.
11. "**Limit**" is the maximum limit of the value of funds that can be transacted by the Customer.
12. "**Login**" is the process of the Customer entering the Internet Banking and One Mobile applications after the Customer enters User ID and Password.
13. "**Logout**" is the process of the Customer leaving the Internet Banking and One Mobile applications after the Customer pressing the logout button that is displayed on the screen.
14. "**Customer**" is the subject of personal law (individuals) or non-individuals, business entities or legal entities based on the prevailing laws and regulations in Indonesia and in accordance with the terms

and conditions of the Bank to become a holder of a savings account, term deposit, current account and/ or credit card at the Bank.

15. "**User Customer**" means a Customer who has been registered as a user of e-Banking Services.
16. "**Call Centre Card Number**" is 16 (sixteen) digit numbers contained in the Call Centre Card.
17. "**Identification Number**" are numbers that are used by the Customer as a Financial Transaction such as account number destination/transfer between OCBC NISP, customer ID number, credit card number/ loans or mobile phone numbers, and others.
18. "**GSM Operators**" is a provider of cellular mobile network/telecommunications services (Global System for Mobile Communication/ GSM).
19. "**Password**" is the Customer identification code or a password that must be inputted by the Customer each time accessing e-Banking Services. In the General Terms and Conditions of e-Banking Service, Password consists of:
    a. E-Statement password is a password that must be inputted by every Customer who will access the e-Statement Service;
    b. Internet Banking/ONe Mobile password is a Password that must be inputted by the Customer who will access the Internet Banking/ONe Mobile service. This Internet Banking/ONe Mobile password is obtained by the Customer after registering the Internet Banking/ONe Mobile and is used for Login.
20. "**PIN (Personal Identification Number)**" is a combination of numbers that are confidential and only known and owned by the Customer. In the General Conditions of e-Banking Service, the PIN consists of:
    a. **Cash PIN** is a PIN for Customers who use OCBC NISP ATM cards;
    b. **Non-Cash PIN** is a PIN for Customers to be used on the OCBC NISP Call or OCBC NISP SMS service;
    c. **Token PIN** is a PIN that is used by a Token holder as a Token access code.
    d. **Transaction PIN** is a password stored in the application for Customer approval prior to carrying out a transaction, which is done through ONe Mobile.
21. "**Main Account**" is the main account used as an OCBC NISP ATM card relation account for transactions including purchases, payment transactions, transactions through other banks' ATM and charging service fees.
22. "**OCBC NISP SMS**" is the Bank's distribution channel to access accounts owned by Customers through SMS (Short Message Service) messages by means of mobile phones.
23. "**SMS**" is a short text transmission that can be sent and or received through a mobile phone and can be viewed through a mobile phone screen.
24. "**SMS Token**" is a transaction authentication code used by the Customer to conduct Banking Transactions through One Mobile which is sent in the form of SMS.
25. "**Expiration Date**" is the end date of a Periodic Transaction that is arranged by the Customer.
26. "**Token**" is the hardware used in transactions through Internet Banking or SMS Token used in transactions through ONe Mobile to enter the transaction authentication code/One Time Password (OTP).
27. **"ONe Mobile**" is a Mobile Banking application owned by the Bank which can be downloaded from PlayStore (for Android smartphones) and the App Store (for iOS smartphones).

28. **"ONe Wallet"** is a server-based electronic money product that is used as a payment instrument issued on the basis of the value of money that is deposited in advance to the issuer. ONe Wallet is not categorized as a deposit (third party fund).
29. **"OTP (One Time Password)"** is a secret code with a six digit number format that will expires in 60 seconds since it is received by the Customer through SMS to a mobile phone number with an active card/SIM Card registered at the Bank, which shall be use to verify access to a mobile phone and carry out PIN activation Transaction on ONe Mobile.
30. **"RM Mobile"** is a platform owned by the Bank that can be carried in mobile by a relationship manager of the Bank to help Customer carry out buying and placing funds on Products of the Bank, including selecting Services and carrying out banking activities.
31. "**Inter Currency Transactions (Cross Currency)**" is a financial transaction in the form of transfer between two accounts with different currencies whereas one of them is an account denominated in Indonesian Rupiah (IDR).
32. "**Periodic transactions (*recurring* or *auto-debit*)**" is a transaction that is instructed by the Customer at present but will be carried out repeatedly in the future for a certain period of time according to the arrangement made by the Customer for the period of time of execution of the transaction.
33. "**Financial Transactions**" are transactions through e-Banking Services involving Customer's funds, which include but are not limited to interbank transfers/ transfers between OCBC NISP, payments and purchases.
34. "**Banking Transactions**" are all transactions conducted by the Customer with the Bank, both Financial Transactions and non-financial transactions.
35. "**Future Date Transactions (future dated)**" are transactions instructed by the Customer at the present but will be executed in the future according to the arrangement made by the Customer on the timing of execution of the transaction.
36. "**User ID**" is a Customer Identification which is used on an Internet Banking/ONe Mobile services which is obtained after the Customer made a registration.

B. PIN, User ID, Password, Transaction PIN and OTP

1. PIN, Password, User ID, Transaction PIN and OTP are confidential and everything associated with the PIN, Password, User ID, Transaction PIN, OTP and all legal actions (transactions) that are associated with it is entirely the responsibility of the Customer, including for any misuse of PIN, Password, User ID, OTP and Transaction PIN.
2. PIN, Password, User ID, Transaction PIN and OTP may only be used by the Account holders who have been approved by the Bank to use an e-Banking Services. User Customer is responsible for maintaining the confidentiality and security of PIN, Password, User ID, Transaction PIN and OTP, among others by:
   a. not notifying or providing User ID, Password, PIN, Transaction PIN and OTP to other person for any purpose including family members or friends;
   b. not writing down or storing User ID, Passwords, PIN, Transaction PIN and OTP in a written form at a place or other means of storage that is likely to be known by others;
   c. User ID, Password, PIN, Transaction PIN and OTP must be used confidentially and not visible to others;

d. not using a PIN, Password, or Transaction PIN that is easily known, such as the date of birth or its combination, telephone number, and others.
e. using a personal communication devices and electronic media and not using communication devices and electronic media that are used or accessed by many people to access e-Banking Services that uses PIN, Passwords, Transaction PIN or OTP;
f. requires changing Password for the first time of using e-Banking Services and change Password, PIN, or Transaction PIN periodically, except for certain e-Banking Services that do not require changing Password, for example e-Statement Services.
g. Avoid using the same PIN, Password, or Transaction PIN repeatedly.

3. User Customer are required to immediately change the PIN received from the Bank.
4. If the User Customer forgot the PIN, User ID, password login on Internet Banking or ONe Mobile, then the User Customer can contact the private banker personnel on the day and business hours.
5. The changing of User ID or Password on the Internet Banking or ONe Mobile will change the User ID or Password on both services.
6. If the User ID, Password, PIN, Transaction PIN and OTP are suspected to have been known or used by other party, the User Customer must immediately report to the Bank for blocking. Failure of the User Customer to report, the User Customer accept the full responsibility for any consequences on the misuse of the User ID, Password, PIN, Transaction PIN and OTP by third parties.

C. Registration

1. If required by the Bank, the Customer must submit the Bank Facility Form (which can be obtained at the Bank branch office), which has been filled out and signed by the Customer. If the Customer is not an individual or a business entity or a legal entity, therefore the opening of account shall be carried out by a person who is authorized to represent the Customer in accordance to legal documents and to completion of data that is required by the Bank.
2. Changes in User Customer data can only be made directly by the User Customer. To non-individual Customers or in a form of business entity or legal entity, changes in User Customer data can only be made by the authorised person to represent the User Customer (specifically).

D. Implementation of Transactions by the Bank

1. The limits of each of the e-Banking Service transactions follows the Limit requirements applicable to each of the e-Banking Services. The Bank in its sole discretion has the right to at any time change the Limit value for each of the e-Banking Service transactions.
2. The Bank has the right to not implement the Customer's Instruction if:
   a. The balance of the Customer's Account is insufficient;
   b. The e-Banking Service is blocked or being blocked for whatever reason;
   c. A system error is occurred.
3. The Customer is responsible for the accuracy and completeness of Instruction in each of the transaction. Any mistakes or failure in issuing the Instruction shall be the full responsibility of the Customer.

E. Account Debit Fees and Authority

1. The transaction fees of E-Banking Service follow the provisions on transaction fees prevailing at the Bank.
2. SMS fees of OCBC NISP follow the fees provisions of each of GSM Operators.
3. The Customer agrees that the Bank has the right to debit transaction fees, administrative fees (if any), Token fees or other fees charged by the Bank, therefore the Customer hereby authorises the Bank to debit the Customer's account at the Bank for payment of the fees. If the e-Banking Service facility is ended, the approval of debiting the relation account for automatic debiting will also ended as long as the Customer has fulfilled all of the obligations.
4. The Bank, with notification to the Customer, can change the fees that must be paid by the Customer as stated in the General Terms and Conditions of the e-Banking Services. The amendment will be notified to the Customer through a media deemed good by the Bank while still observing provisions of the prevailing laws and regulations of the Republic of Indonesia.

F. Termination of Services

Each of the e-Banking Services shall end upon the submission by the Customer to the Bank, an application to close a facility or relation account used for debiting.

2. SPECIAL PROVISIONS IN RELATION TO SERVICES

A. OCBC NISP ATM Card

1. Requests for issuance, activation and amendment to OCBC NISP ATM card facility must be based on a request from the Customer and approved by the Bank.
   Customers who hold a Joint Account "And" shall not receive an OCBC NISP ATM card, while Customers who have a Joint Account "Or" can receive an OCBC NISP ATM card provided that it is issued only to the first Customer named in the Joint Account. Customers with "Or" Joint Account are jointly liable for all risks arising from the use of the OCBC NISP ATM card as stipulated in the General Terms and Conditions of the e-Banking Services.
2. Fees and daily limit of transactions at Bank OCBC NISP ATM shall follow the prevailing provisions at the Bank and a more detail information on this matter can be viewed at *https://www.ocbcnisp.com/personal-banking/Jasa-Layanan/Jasa-Perbankan/Info-Tarif-Biaya.aspx.*
3. The Card can be used at all OCBC NISP ATMs, OCBC NISP EDCs, ATMs or EDCs which cooperate with the Bank and other electronic transaction facilities provided by the Bank.
4. Every transaction through OCBC NISP ATM, OCBC NISP EDC, ATM or EDC which cooperate with the Bank and other electronic transaction facilities provided by the Bank is regulated with daily Limit according to the provisions determined by the Bank or ATM or EDC which cooperate with the Bank based on prevailing regulations.
5. For transactions conducted at ATMs or EDCs and other electronic transaction facilities which cooperate with overseas Banks and/or in foreign currencies, the transaction value shall be converted by the Bank into Rupiah based on the prevailing exchange rate at the time of transaction or according to procedures determined by the Bank.
6. The Customer can provide Instructions to block OCBC NISP ATM card through the Call OCBC NISP service or branch offices of the Bank.
7. The Customer may submit a request for replacement of the OCBC NISP ATM card to the Bank and the Customer agrees to bear all administrative costs(s) incurred. With the issuance of the new OCBC

NISP ATM Card, the previous OCBC NISP ATM Card shall become invalid.

8. The Customer shall be fully responsible for any loss arising due to the loss of OCBC NISP ATM Card or misuse or transfer of OCBC NISP ATM Card as a result of an error or negligence of the Customer.

B. Internet Banking and ONe Mobile

1. Internet Banking and ONe Mobile facility are only intended for individual Customers.
2. Registration of Internet Banking and ONe Mobile
   a. Every Customer who requires Internet Banking/ONe Mobile facilities can register through:
      1. ATM OCBC NISP, in which the Customer will receive a User ID and Password;
      2. Branch offices of the Bank, by completing the Bank Facility Form and attaching proof of photocopy of Identity of the Customer and other required documents, subsequently the Customer will receive a User ID from the customer service officer, while the Password shall be sent to the Customer's e-mail address. If the Customer does not receive a Password within 2 (two) calendar days, the Customer shall commence re-registration.
      3. ONe Mobile, which can be downloaded from the App Store and Play Store. ONe Mobile user can create a user ID, Password, PIN and Transaction PIN when registering the ONe Mobile.
      4. For opening a new account through RM Mobile, the Customer will received a user ID and Password for Internet Banking and ONe Mobile when opening an account and registering as a new Customer.
   b. After the Customer receive the User ID and Password for the first time, then no later than 2 (two) calendar days from the receipt of the User ID and Password, the Customer is required to Login and change the Password. If during this period the Customer does not Login to Internet Banking, the Customer must commence re-registration.
   c. Orders/Instructions provided by the Customer can only be done/provided to the Bank through the Customer's mobile phone number registered at the Bank.
   d. The Customer must update the mobile phone number if there is any changes to the Customer mobile phone number which will be used to make a transaction in ONe Mobile through ATM or OCBC NISP EDC.
3. Transactions Using Internet Banking and ONe Mobile
   a. To conduct Financial Transactions through Internet Banking and ONe Mobile, the Customer must first have a User ID, Password, Token, PIN or Transaction PIN.
   b. As a sign of approval of a Financial Transaction instruction and as an authorisation of a Financial Transaction, the Customer must enter the Response Code from the Token or Transaction PIN.
   c. In every Financial Transaction, the system will always confirm the data entered by the Customer and the Customer has the opportunity to cancel the data by pressing the "Cancel" or *"Batal"* button.
   d. Every information that receive a "Submit" or *"Kirim"* confirmation from the Customer which is stored at the Bank's

data centre, shall be the correct data and as evidence of a valid instruction from the Customer to the Bank to carry out the transaction.

e. Transactions that have been confirmed "Submit" or *"Kirim"* by the Customer and have been authorised using the Response Code from the Token or Transaction PIN (for Financial Transactions) cannot be cancelled.

f. For Future Date Transactions of a Financial Transactions through Internet Banking or Periodic Transactions (recurring or auto-debit), the Customer may cancel the transaction by submitting an authorisation for the cancellation with a Token Response no later than 1 (one) Calendar Day prior to the effective date/due date or expiration date of the transaction.

g. For Future Date Transactions (future dated) or Periodic Transactions (recurring or auto debit), the transaction will be processed at the beginning of the day. For Periodic Transactions, if the Expiry Date falls on the same date as the periodic date specified, then the transaction will still be processed on that day.

h. For Financial Transactions of funds transfer to other domestic bank accounts through Giro Traffic ("LLG"), if the effective date of the transaction falls on a Holiday, the transaction will still be accepted and will be carried out on the following Business Day.

i. For Financial Transactions of funds transfer to other domestic bank accounts through RTGS, if the effective date of the transaction falls on a Holiday, the transaction shall fail.

j. For Financial Transactions of funds transfer to other domestic bank accounts that have online facilities through ATM network in cooperation with the Bank, the transaction shall commence even though it falls on a Holiday.

k. For each successful Financial Transactions instructed by the Customer, the Customer will receive a reference number as proof that the transaction has been carried out by the Bank.

l. Cross-Currency Transactions can only be carried out for types of foreign currencies issued by the system. The Customer cannot request a special exchange rate. The Cross-Currency Transactions are only valid for transfers between Bank accounts.

m. The Limit of payment transaction by using a QR Payment feature in ONe Mobile at a merchant/outlet/store which has a QR Code-based/QRIS logo shall follow the prevailing provisions at the Bank and detailed information on this matter can be viewed at *https://www.ocbcnisp.com/personal-banking/Landing/ONe-Mobile/FAQ-ONe-Mobile.aspx#qris.*

n. Transactions carried out by the Customer on ONe Mobile or Internet Banking are recorded by the Bank system and recorded on the mutation of the Customer's account at the Bank.

o. The Customer is required to log out every time the Customer finishes or no longer use the Internet Banking and ONe Mobile.

4. Electronic Mail (e-mail)

a. Every Customer will receive 1 (one) message in the "Mailbox" of the Internet Banking or ONe Mobile application. The Mailbox is used by the Customer to receive transaction information that has been carried out by the Customer through Internet Banking or ONe Mobile.

b. In addition to the Mailbox referred to in point a above, the Customer can receive information about transactions that have been carried out by the Customer on Internet Banking or ONe Mobile through the e-mail address registered by the Customer when opening an account or registering for Internet Banking or ONe Mobile services.
c. The Bank will send information about Internet Banking or ONe Mobile transactions in accordance with Customer's request to the Customer's personal e-mail address. The Bank is not responsible for the non-receipt of such information due to incorrectness or changes in Customer's personal e-mail address which has not being reported to the Bank.
d. The Bank does not guarantee the security of information or data sent to the Bank through the Customer's personal e-mail address.

5. Blocking of Internet Banking and ONe Mobile Password
   a. The Customer's password will be blocked if:
      1. Errors occurred in entering the Password of 3 (three) times continuously at Login;
      2. The Customer requested the Bank to block the Password.
   b. In the event of a Password blocking, the Customer is required to reset the Password by contacting the private banker personnel on the day and business hours.
6. Terms and Conditions for Token Holders for Internet Banking and ONe Mobile
   a. Customers who require Token must register and have a current or savings account or a credit card at the Bank.
   b. Registration of Token/Transaction PIN:
      1. Token registration for the Internet Banking facility is carried out through Internet Banking and submitting a print out of the Token order application at the time of collection of the Token at the Bank branch.
      2. PIN Registration Transaction is carried out at time of registration through ONe Mobile.
   c. Internet Banking Tokens are owned by the Bank and must be returned to the Bank immediately upon request by the Bank.
   d. Internet Banking Tokens and ONe Mobile are only to be use by the Token holders themselves and cannot be transferred in any way to anyone.
   e. The Internet Banking Tokens and ONe Mobile cannot be used for purposes other than for transactions that have been determined by the Bank.
   f. The Internet Banking Token holders are required to maintain good condition of the Token including but not limited to battery replacement of Token. The cost of replacing the battery is fully borne by the Customer.
   g. The bank will provide Token PIN to Internet Banking Token holders.
   h. The blocking of Internet Banking Tokens and ONe Mobile
      1. In the event the holder of the Token or Transaction PIN had incorrectly enters the Token PIN 3 for (three) times continuously, then the Token will be automatically blocked.
      2. In the event that an Internet Banking Token or a mobile phone receiving SMS Token is stolen or lost or is suspected of being misused by another party, the Token holder must immediately block the Token by

contacting Call OCBC NISP or the nearest Bank branch office.

i. Reset of Token and Transaction PIN, New Internet Banking Token and ONe Mobile application
   1. If the Token and Transaction PIN were auto blocked, the Token holder can reset the Token or Transaction PIN through the nearest Bank branch office or Call OCBC NISP.
   2. In the event that a Token is lost or stolen or is suspected of being misused by another party, then after blocking, the Token holder can submit a new Token application through the nearest Bank branch office by filling in the Bank Facility Form and submitting the original loss report from the local police at the latest within 2 (two)) Business Day after the loss event. The Bank is acquitted from all claims, damages and lawsuit if the Customer fails to report within the timeframe set out above.

j. As long as the Token or Internet Banking and ONe Mobile Transaction blocking has not been done by the Token holder, the Bank will not be responsible for any transactions made using the lost/stolen Token.

k. In the event that the Internet Banking Token is damaged, the Token holder must report it to the Bank and submit the damaged Token to be replaced.

l. All transactions made using Token, whether used with or without the knowledge of the Token holder regardless of its use, are the full responsibility of the Token holder.

m. Complaints and/or objections from the Token holder can only be responded by the Bank if a complaint and/or objection of the use of a Token is submitted to the Bank within a period of 3 (three) months from the date the transaction is made.

n. For joint account holders with a single transaction authorisation "Or", the Bank can only provide the Token to one of the joint account holder name in accordance to a written agreement made by all of the joint account holders.

o. The Bank at any time has the right to block, cancel, withdraw or renew the Internet Banking Token if the Token holder has no longer meets the terms and conditions of a Token holder.

p. If an Internet Banking Token holder wishes to stop using the Token, the Token holder must notify the Bank in writing and the Token must be returned to the Bank. The termination of the use of the Token is effective from the date of the notification made and signed by the Token Holder is received by the Bank.

q. As long as the Internet Banking Token has not been activated, then the Token holder can still conduct non-financial transactions on Internet Banking.

r. If the Internet Banking Token is has not been collected within 3 (three) months from the request is submitted, the Token cannot be provided to the Customer, therefore the Customer is required to make a re-registration.

s. In the event the Bank receives information that the individual Token holder has deceased, the Token facility shall be terminated by the Bank. As long as the Bank has not received notification of the deceased of the individual Customer, the use of the Token is outside of the Bank's responsibility.

C. e-Statement

1. The Customer must (a) have and register the Customer's personal e-mail address with the Bank, (b) ensure that the e-mail address is correct and is the property of the Customer; and (c) has all the software needed to use the e-Statement Service, including to anticipate interference in any form (including but not limited to virus, bug, malware) so as not to cause interference in any form to the computer system of the Customer and the Bank. The Customer hereby releases the Bank from all responsibility for risks arising from the use of the e-Statement Service from the Bank.
2. Transaction Data will be sent by the Bank from the Bank e-mail to the Customer e-mail that has been registered on the Bank system, at the beginning of each month on a Business Day. Data transmission will be carried out by the Bank 1 (one) time and if a delivery failure occurs, the Bank may resend it to the Customer. The resending of the Transaction Data will be carried out by the Bank to the e-mail address of the Customer registered on the Bank system. If the Customer wishes to register a new e-mail address as the registered e-mail, the Customer can directly register it at the Bank's account opening branch office.
3. The Customer acknowledges and agrees that if an e-Statement Service is approved by the Bank, the Customer may not request the Bank to reprint the Transaction Data on the e-Statement to a current account form to be sent by a registered post. If the Customer requires the Bank to revert back to a current account form, then the Customer shall submit changes of data to the Bank's account opening branch office and further the Bank may change the delivery of the Customer Transaction Data through a current account by a registered post on the next month.
4. Termination of e-Statement Service or changes to Customer's e-mail address can be made by submitting a written request to the Bank that has been filled and signed by no later than 5 (five) Business Days before the end of the month through the nearest Bank branch or contacting Call OCBC NISP. Changes to e-mail addresses will be effective on the following month of the e-Statement delivery. The Customer agrees and authorises the Bank to terminate the e-Statement Service if the data and documents including the e-mail address provided by the Customer to the Bank are incorrect, inaccessible, incorrect writing or any cause that results in failure of the implementation of the e-Statement Service which is not caused by mistake and/or negligence of the Bank. All consequences and risks arising from changes in e-mail addresses are the responsibility of the Customer.
5. In the event of any difference between the Transaction Data listed on the e-Statement and the Transaction Data listed on the Bank's records, the Customer agrees that the Transaction Data recorded at the Bank is the valid and binding to the Bank and the Customer, unless the Customer can prove otherwise.

D. ONe Wallet

1. ONe Wallet registration can be submitted by Customers and non-Customers, by downloading the ONe Wallet application on Google Playstore for Android users or Apple App Store for iOS users.
2. Activation of ONe Wallet is carried out by filling out and completing data as required by the Bank with unregistered status.

3. Every ONe Wallet user must follow the Customer Due Diligence (CDD) process as determined by the authorised regulator and refer to the Policy of Anti-Money Laundering and Prevention of Terrorism Financing (APU-PPT) of the Bank.
4. For the establishment of ONe Wallet user profile as part of the CDD process, ONe Wallet users are divided into 2 (two) and are required to provide data and information as follows:
   a. Registered
      The information needed is: name, identity number, address of residence according to identity card (KTP), address of another residence/domicile if available, place and date of birth, nationality, telephone number in the form of mobile number, e-mail address, occupation, gender, and signature/biometric data. The information must be supported by documents, namely KTP/SIM/PASSPORT.
   b. Unregistered
      The information needed is: name, identity number, address of residence according to identity card (KTP), place and date of birth, telephone number in the form of mobile phone number and email address. This information is not required to be supplemented with supporting documents.

   The user is obliged to ensure that the e-mail address provided to the Bank is correct and fully the property of the user.
5. The value of money deposited into ONe Wallet can be used or transacted in full until it is zero in balance.
6. Funds stored in ONe Wallet are not included in the category of Third Party Funds (DPK). With the use of ONe Wallet, the ONe Wallet users agree that the value of the money deposited is not guaranteed by the Deposit Insurance Corporation and shall not incur interests on its deposits by the Bank.
7. The complete terms and conditions of ONe Wallet can be viewed or downloaded at https://www.ocbcnisp.com/id/digital-channel/one-wallet in section "Terms and Conditions". Upon the Customer agreeing to these Terms and Conditions, the Customer is subject to and bound to the ONe Wallet Terms and Conditions including its amendments and/ or renewals in the future.
8. ONe Wallet user (both Registered and Unregistered) can use the QR Payment on ONe Wallet application to make payment transactions at any merchants / outlets / stores that have QRIS logo with limits following the applicable provisions at Bank. Detailed information about the QR Payment or QRIS can be seen on the website https://www.ocbcnisp.com/id/faq on the Digital Channel / ONe Wallet section. For questions or further information, ONe Wallet user can contact call OCBC NISP at 1500-999 or visit www.ocbcnisp.com

E. Call OCBC NISP

Business customers, individual customers and non-customers can use Call OCBC NISP services through communication media determined by the Bank from time to time. Services for customer requests related to accounts, confidential and transactional data, must be verified in advance by the Call OCBC NISP team in accordance with regulations of the Bank. In the event that the Bank cannot verify in accordance with the prevailing provisions at the Bank, the Bank has the right not to continue/follow up the Customer's request.

Specific for Business Customers

1. Business Customers (business banking) can use Call OCBC NISP service by selecting menu 2 for Business Customer Services;

2. Business Customer Services can use Indonesian or English according to the Customer's choice menu;
3. Furthermore, the Customer can choose banking products in the IVR application as desired and directly handled by the Business Banking Contact Centre Team.

Interactive Voice Response (IVR)

1. Registration of Call OCBC NISP Transaction Identification Number
   Every individual customer who needs a Financial Transaction via IVR can register at one of the nearest Bank branches, by writing down the Identification Number to be used to carry out a Financial Transaction on the Bank Facility Form provided by the Bank.
2. Transactions Using IVR
   To be able to use Financial Transactions through IVR, the Customer must enter the OCBC NISP ATM card number and PIN to be verified by the system.
   1. In the event that the Customer will carry out a Financial Transaction, then the Financial Transaction can be carried out if the Identification Number has been registered in the Bank system.
   2. The Customer has the opportunity to cancel the Financial Transaction that has not been done by pressing the number "0" (zero). Financial Transactions that have been successfully carried out by the Customer cannot be cancelled.
   3. For each successful Financial Transaction, the Customer will receive proof of the transaction in the form of a transaction code.

F. OCBC NISP Autopayment

1. The Customer agrees to make the account into a relation account for automatic debiting of a routine transaction through the Autopayment facility ("Relation Account") and agrees to authorise the Bank to conduct automatic debiting of the Relation Account including costs for the implementation of the Autopayment facility. The amount of this fee will be determined by the Bank.
2. The Customer is responsible for providing funds in the Relation Account for the implementation of the Autopayment facility no later than 1 (one) Business Day prior to the last payment date in accordance with the provision of the biller.
3. In the event that the Relation Account is closed due to any reason, the Customer is obliged to replace it with a new relation account. If the Customer does not replace the closed Relation Account, the Autopayment facility will be automatically terminated by the Bank.
4. The Customer agrees that the Bank is not responsible for failure in debiting because (i) unavailability of the billing data; (ii) insufficient funds in the Relation Account, or the termination of the Autopayment facility for any reason; or (iii) Customer's mistakes or negligence in implementing the General Terms and Conditions of e-Banking Services and other applicable provisions at the Bank including its amendments;
5. If the Customer intends to terminate the Autopayment facility, the Customer must notify the Bank in writing of the start of the termination and submit it by no later than 7 (seven) Business Days prior to the start of the payment period for the relevant Autopayment facility.
6. The Customer is responsible for filling out and signing the new Bank Facility Form and submitting it to the Bank in the event that a Relation Account number has changed.

G. Automatic Fund Transfer

1. The Customer agrees to have the account registered as a relation account for debiting an Automatic Fund Transfer transaction.
2. The Customer authorises the Bank to debit the Automatic Fund Transfer for the relation account.
3. If at the payment due date of, the implementation of Automatic Fund Transfer cannot be carried out by the Bank due to Customer's negligence or error, the Bank is released from any risks and claims.
4. In the event of a closure of a relation account by the Bank due to Customer's negligence or error, the Customer promises to replace it with a new relation account. If the Customer does not replace the closed relation account, the Bank will stop this facility.

H. OCBC NISP SMS

1. Registration and Changes of Customer Data for OCBC NISP SMS Facility
   a. For registration of the OCBC NISP SMS facility, the Customer is required to submit 1 (one) Primary Account number.
   b. The Main Account must be equipped with OCBC NISP ATM facility.
   c. If the Main Account is closed, then to avoid the failure of the OCBC NISP SMS transaction, the Customer must replace the Main Account.
   d. If the Customer has fulfilled the requirements then as a sign of approval, the Bank will provide an OCBC NISP SMS PIN to be sent directly to the mobile phone of the User.
2. Terms of Use of OCBC NISP SMS
   a. The OCBC NISP SMS service can be used by the User Customer to obtain information and commence selected/ registered banking transactions.
   b. Matters that must be considered in every transaction that is carried out through the OCBC NISP SMS facility are:
      1. Transactions can be carried out on all accounts related to OCBC NISP ATM, both the Main Account and additional accounts.
      2. The User Customer must ensure the accuracy and completeness of transaction instructions, including the correctness of data on the Bank Facility Form, in accordance with the SMS command format determined by the Bank.
      3. As a sign of approval of the transaction, the Customer is required to fill in the OCBC NISP SMS PIN at the end of each instruction delivery.
      4. Limit of transfer transactions or transfers for the OCBC NISP SMS facility refers to the limit of transfer transactions or transfers attached to the OCBC NISP ATM card, which is a combination of the Main Account and additional accounts.
3. OCBC NISP SMS PIN
   a. Every SMS OCBC NISP User Customers are given 1 (one) PIN number issued with the Bank on a system basis.
   b. The PIN will be sent through SMS message to the Customer's mobile phone registered with the Bank by no later than 1 x 24 (twenty-four) hours after registration, either registration being conducted at the OCBC NISP ATM or at the branch office.
   c. The User Customer must replace the PIN received from the Bank with a new self-made PIN when using the OCBC NISP SMS service for the first time.

d. PIN replacement can be done through SMS.

4. Miscellaneous
   a. Evidence of the User Customer's instruction made through the OCBC NISP SMS service is the account mutation which can be seen in the current account or savings book.
   b. If there are problems relating to mobile phone numbers, GSM networks, GSM usage bills, SMS fees and GSM value added services, the User Customer shall directly contact the GSM Operator concerned.
   c. The User Customer can contact the customer service of the Bank or Call OCBC NISP for any issues relating to transactions and changes of access to OCBC NISP SMS services.

The General Terms and Conditions of the e-Banking Services including all of its amendments and or renewals ("**General Terms and Conditions of e-Banking Services**") constitute one and inseparable part of (i) Bank Facility Forms including its terms and conditions, (ii) general terms and conditions relating to each of the Bank related products, and (iii) Terms and Conditions of Account Opening and Arrangement of PT Bank OCBC NISP, Tbk.

This General Terms and Conditions of e-Banking Services can be changed at any time by the Bank with notification to the Customer through a media deemed good by the Bank subject to the prevailing laws and regulations.

In the event that these General Terms and Conditions of e-Banking Services is translated in another language, any discrepancy or conflict between the Indonesian language and the foreign language of the text, the Indonesian language text shall prevail.

THESE GENERAL TERMS AND CONDITIONS OF E-BANKING SERVICES HAVE BEEN ADJUSTED TO BE IN ACCORDANCE WITH THE LAWS AND REGULATIONS INCLUDING THE REGULATIONS OF THE FINANCIAL SERVICES AUTHORITY.