BANK MESTIKA

TERMS AND CONDITIONS
INDIVIDUAL INTERNET BANKING AND MOBILE BANKING
PT BANK MESTIKA DHARMA TBK

A. DEFINITION

1. Bank is PT Bank Mestika Dharma Tbk.
2. The Customer is the party using the services of the Bank and has a savings account in the form of a checking and/or savings account with the Bank.
3. The Bank Customer has registered as an Internet Banking and Mobile Banking User.
4. Individual Internet Banking, hereinafter referred to as Internet Banking, is the utilization of Internet technology used by Bank as a platform for Customers to conduct various banking transactions through a web browser application.
5. Mobile Banking is a service that allows Individual Bank Customers to perform a variety of financial transactions through mobile devices such as smartphones or other gadgets.
6. Mobile Token is a software program within the Mestika Mobile application used to authenticate transactions from Bank Mestika's Internet Banking.
7. Mestika Mobile is a Mobile Banking and Mobile Token Internet Banking service that offers speed and convenience in banking transactions, both financial and non-financial, through smartphones or other gadgets.
8. Quick Response Code for Payment, hereinafter referred to as Payment QR Code, is a two-dimensional code consisting of markers of three squares patterns at the bottom-left, top-left, and top-right corners. It features black modules in the form of square dots or pixels and has the capability to store alphanumeric data, characters, and symbols. It is used to facilitate contactless payment transactions through the scanning of QR Codes.
9. The National Standard for Payment QR Code (Quick Response Code Indonesian Standard), hereinafter referred to as QRIS, is the standard for Payment QR Code established by Bank Indonesia for use in facilitating payment transactions in Indonesia.
10. QRIS-QR Payment transactions refer to payment transactions on Mobile Banking services facilitated by scanning Payment QR Codes based on QRIS. These include both Static Payment QR Codes and/or Dynamic Payment QR Codes provided by Merchants in Indonesia.
11. The Bank only acts as the Payment Service Provider (PJP) Issuer for the QRIS-QR Payment feature, hereinafter referred to as PJP Issuer. The PJP Issuer conducts fund source management activities (account issuance services) as stipulated in the regulations of Bank Indonesia that govern payment systems and payment service providers.
12. The National Merchant Repository, hereinafter abbreviated as NMR, is a system with the capability to manage and organize data related to merchants.
13. QRIS Merchants, hereinafter referred to as Merchants, are providers of goods and/or services registered in the National Merchant Repository (NMR) to accept QRIS-QR Payment transactions.
14. Static Payment QR Code is a Payment QR Code issued before any transaction is initiated. It can be scanned repeatedly to facilitate various different payment transactions. Typically, it only contains information about the identity of the merchant (Merchant).
15. Dynamic Payment QR Code is a Payment QR Code issued after a transaction is initiated. It is scanned to facilitate a specific transaction and usually contains information about the identity of the merchant (Merchant) or the user and details about the transaction, such as the transaction amount.
16. The User ID is an identity created by the Customer during registration, consisting of a combination of letters and numbers (alphanumeric) with a length of 6 (six) to 12 (twelve) characters, and is used for Internet Banking and/or Mobile Banking services.
17. The Internet Banking and Mobile Banking Password, hereinafter referred to as Password, is a personal and confidential passphrase created by the Customer, consisting of a combination of letters and numbers (alphanumeric). It must include at least one capital letter and special characters (! @ % * _ + - = . ,) with a length of 8 (eight) to 12 (twelve) characters and is used for Internet Banking and/or Mobile Banking services.
18. The Mobile Token PIN (Personal Identification Number), hereinafter referred to as PIN, is a series of numbers (consisting of 6 digits) created by Customers during the activation of Mobile Token. It is personal and

confidential, known only to the Customer. The PIN is used for Mobile Token services and Mobile Banking transactions.

19. Challenge Number is a sequence of numbers (comprising 10 digits) displayed on the confirmation page when Customers intend to perform Internet Banking service activities. Customers are required to enter it into the Mobile Token to obtain a Response Code, which will be entered into the available response column.
20. Response Code is a sequence of 10 (ten) digits that serves as a one-time secret code generated by the Mobile Token and is used to authenticate every Financial and Non-Financial Transaction made through Internet Banking.
21. The OTP Code is a 4 (four)- digit number obtained by Customers during the registration of Internet Banking services on the Internet Banking Bank Mestika website https://ib.bankmestika.co.id. It is also sent to Customers during the activation of the Mobile Token and registration for Mobile Banking services.
22. The Information Service (Inquiry) is a service provided by the Bank to Customers in the form of general information about transaction deadlines, foreign exchange rates and transaction history.
23. Banking Transactions consist of non-financial transactions and financial transactions.
24. Non-Financial Transactions are information services in the form of transactions that do not affect the account balance.
25. Financial Transactions are services provided by the Bank to Customers in the form of transactions that impact the account balance.
26. The Financial Transaction Limit is the maximum nominal limit for a transaction that can be provided by the Bank, in accordance with applicable laws and regulations as well as the Bank's internal policies.
27. The Primary Account is the account in the name of the User Customer that is active and is the first account registered in Internet Banking and Mobile Banking services for the debiting of fees in accordance with the Bank's internal policies.
28. The Account List is all the account numbers owned by the Customer, registered and accessible by the Customer.
29. The Notifications service sends SMS messages for OTP codes and emails for both successful and unsuccessful transactions conducted by Customers through Internet Banking and Mobile Banking.
30. Facilities encompass all the services available within Internet Banking and Mobile Banking, which may change at any time in accordance with the bank's internal policies.
31. Maximum Retry refers to a maximum of 3 (three) password attempts by the Customer before being locked by the system.

B. ACCOUNT

1. Accounts eligible for registration in the Internet Banking and Mobile Banking service must be individual or personal accounts (not joint accounts).
2. The account types eligible for registration as the Primary Account in the Internet Banking and Mobile Banking service are savings accounts such as "Tabungan Mestika" and/or checking accounts, which have an ATM card.
3. Accounts other than "Tabungan Mestika" and/or Checking accounts are automatically registered in Internet Banking and Mobile Banking as additional accounts for informational purposes.
4. The Primary Account and other accounts registered in Internet Banking and Mobile Banking belong to the accounts under one Customer Identification Number (CIF).
5. The accounts displayed on Internet Banking and Mobile Banking are those registered with the Bank, and do not include joint accounts or Digital Banking MiND by Bank Mestika accounts.
6. The maximum deposit amount guaranteed by the Deposit Insurance Corporation (LPS) per Customer at the Bank is IDR 2,000,000,000 (two billion rupiahs).
7. Information on the guarantee interest rate can be accessed via https://apps.lps.go.id/BankPesertaLPSRate.
8. The Customer hereby grants the Bank the right and authority to delay transactions, temporarily suspend transactions, block the account, reject transactions, and/or close the account, in the event that:
   a. the Customer fails to comply with applicable laws and regulations;
   b. the Customer fails to provide information and supporting documents in accordance with applicable laws and regulations;

c. the Customer is known and/or reasonably suspected to have used forged documents and/or provided incorrect or false data/information to the Bank;
d. the Customer provides information whose accuracy is questionable;
e. the Customer has transaction funds whose source is known and/or reasonably suspected to be derived from the proceeds of a criminal offense;
f. the Customer is known and/or reasonably suspected of holding an account used to receive, store, or manage assets derived from the proceeds of a criminal offense;
g. there is an order from a regulator or other authority having the power to do so under applicable laws and regulations;
h. the Customer, including the Beneficial Owner, is listed in the List of Suspected Terrorists and Terrorist Organizations and/or the List of Proliferation Financing of Weapons of Mass Destruction;
i. the Customer, including the Beneficial Owner, is listed in the List of Parties Suspected of Involvement in Online Gambling and/or the List of Suspected Terrorism Financing;
j. the Customer, including Beneficial Owners, from countries designated as High-Risk Jurisdictions Subject to a Call for Countermeasures according to The Financial Action Task Force on Money Laundering (FATF) publications;
k. Based on the Bank's assessment and/or analytical systems, the Customer conducts suspicious transactions and/or transactions beyond reasonable usage limits and/or transactions categorized as fraud.

C. REGISTERED PHONE NUMBER

1. Customers must ensure that the mobile phone number registered to the Internet Banking and Mobile Banking service is correct.
2. Misuse of the mobile phone number registered to the Internet Banking and Mobile Banking service is entirely the responsibility of the Customer.

D. *ELECTRONIC MAIL (E-MAIL)*

1. Customers are required to register their personal email address for the purpose of receiving successful transactions receipts and all matters relating to the Internet Banking and Mobile Banking service.
2. Customers must maintain the confidentiality of the registered email messages from the Bank.
3. Misuses regarding the email address registered with the Bank for Internet Banking Mobile Banking services are entirely the responsibility of the Customer.

E. INTERNET BANKING AND MOBILE BANKING ACCESS

1. Customers can access the Internet Banking service through the Internet Banking Bank Mestika website at https://ib.bankmestika.co.id.
2. Customers can access the Mobile Banking service through the Mestika Mobile application downloaded on their smartphone/gadget.
3. Customers can access the Internet Banking and Mobile Banking service by entering the User ID and Password correctly.
4. Customers are advised to delete emails and/or SMS notifications from the Bank containing registration data, passwords, changes, or Customer transaction data after reading such emails or SMS notifications.
5. Customers are advised to update the Mestika Mobile application for a more comfortable transaction experience.
6. For security purposes, Customers are advised to not access the Internet Banking and Mobile Banking through free internet service facilities or free Wi-Fi service.
7. Any losses suffered by Customers as a result of using free internet service facilities or free Wi-Fi services as referred to in point 6 above are entirely the responsibility of the Customer.

F. REGISTRATION FOR INTERNET BANKING AND MOBILE BANKING SERVICE

1. Customers can register for the Internet Banking service through the Bank Mestika Internet Banking website at https://ib.bankmestika.co.id.

2. Customers must have a registered email address and mobile phone number at Bank Mestika.
3. All Customer-related data requested by the Bank is used for the purpose of the Bank Mestika Internet Banking and Mobile Banking registration process.
4. For Internet Banking Customers:
   a. Required to have an ATM card.
   b. Input the account number to be used for Internet Banking registration on the verification page.
   c. Will receive a notification via SMS containing an OTP code to the Customer's mobile phone number used during the initial registration as a Bank Mestika customer.
   d. Enter the OTP and verify on the ATM validation page by providing the correct ATM card number, date of birth, ATM card expiration date, correct 6-digit ATM card PIN and captcha. Check the terms and conditions box for Bank Mestika's Individual Internet Banking and Mobile Banking Bank Mestika, then verify.
   e. The ATM card will be automatically blocked if the ATM card PIN is entered incorrectly 3 (three) times.
   f. After verification, the Customer is requested to create an account with 1 (one) User ID and 1 (one) Password that will be used to access the Internet Banking service.
   g. Registration for the Internet Banking service is successful after the Customer successfully creates an account/ User ID.
   h. To obtain the Mobile Token, the Customer must download the Mestika Mobile application from the App Store (for iOS) or Play Store (for Android) on the Customer's smartphone/device after successfully registering for the Internet Banking service.
   i. After downloading the Mestika Mobile application on the Customer's smartphone/device, select the Mobile Token menu for activation. The Customer will then be directed to provide information such as the account number, mobile phone number and ATM card number used during Internet Banking registration.
   j. The Customer will receive an SMS containing an OTP Code. Input this OTP code and the Customer will be prompted to create and confirm a PIN. The Mobile Token is then successfully activated and can now be used to perform Internet Banking transactions.
5. For Mobile Banking Users:
   a. Mobile Banking services can only be utilized if Customers have registered for Internet Banking services and activated the Mobile Token beforehand.
   b. Customers are required to download the Mestika Mobile application from the App Store (for iOS) and Play Store (for Android) on their smartphones/gadgets after successfully registering for Internet Banking services.
   c. Must have a registered email address and mobile phone number at Bank Mestika.
   d. Customers agree and checkmark the Terms and Conditions of Individual Internet Banking and Mobile Banking on the Terms and Conditions page before registering for Internet Banking services.
   e. Register for Mobile Banking services on the Mestika Mobile application by entering the same User ID and Password used for Internet Banking services.
   f. Enter the OTP code received via SMS along with the Mobile Token PIN (6-digit number), then click the verify button to verify the OTP code and Mobile Token PIN. Customers will be directed to the Mobile Banking welcome page, indicating a successful registration.
6. Customers can update their customer information by filling out the Customer Identity Form at the nearest bank office.
7. Customers have read and understood the Terms and Conditions of Individual Internet Banking and Mobile Banking.
8. If an Individual Internet Banking Customer activates Mobile Banking at a later date, the Customer shall remain bound by these Terms and Conditions of Individual Internet Banking and Mobile Banking of Bank Mestika.

G. *USER ID, PASSWORD* AND PIN

1. Customers are free to create their own User, Password, PIN and can make changes or replacements to their Password as desired through the Internet Banking service at https://ib.bankmestika.co.id.
2. Used Passwords can be reused after using 3 (three) different passwords.
3. Customers can use the "Forget Password" feature on the Internet Banking Login page at https://ib.bankmestika.co.id with the Mobile Token if:

a. The Customer forgets the Password.
b. The Customer has reached the Maximum Retry limit of 3 (three) times in a row on the same day.

4. Customers are required to secure their User ID, Password and PIN by:
   a. Not disclosing User ID, Password and PIN to others.
   b. Not writing down User ID, Password and PIN on any media, storing them in written form or other storage methods that could be discovered by others.
   c. Regularly changing the Password.
   d. Advised to not performing Internet Banking transactions on publicly used computers and/or accessing the Internet Banking and Mobile Banking service through free/public internet facilities or Wi-Fi services.
   e. Ensure that the visited website is the official Internet Banking site as informed by the Bank.
   f. Logging out immediately after completing a transaction(s) using the Internet Banking service.
5. The confidentiality of User ID, Password and PIN is entirely the responsibility of the Customer.
6. Do not use PIN combinations that are personal data and easily known by others, such as birthdates.
7. The use of the User ID, Password and PIN has the same legal power as a written order signed by the Customer. Therefore, the Customer states that the use of User ID, Password, PIN in any transaction through Internet Banking and/or Mobile Banking is an authorization given by the Customer to the Bank to conduct transactions.
8. Customers are advised to contact the Bank's Call Center or the nearest Bank's Customer Service to block the User ID if the Customer's smartphone/device is lost, transferred to another party, etc.
9. The Bank is exempt from any legal claims if there is a misuse of User ID, Password and PIN by irresponsible parties because of the Customer's negligence.

H. MOBILE TOKEN

1. The Mobile Token can only be used by the Customer.
2. Customers can obtain the Mobile Token by downloading the Mestika Mobile application from the App Store (for iOS) or Play Store (for Android).
3. Customers are required to use the Mobile Token for authentication in Financial and Non-Financial transactions.
4. The Mobile Token cannot be used for other purposes outside of authenticating Financial and Non-Financial transactions specified by the Bank.
5. The Bank is exempt from any legal claims if there is a misuse of the Mobile Token by irresponsible parties because of the Customer's negligence.

I. TRANSACTIONS

1. Customers must provide or fill in all required data for each transaction accurately and correctly.
2. The system will always confirm the data recorded or provided in the Internet Banking and Mobile Banking Service for every Financial transaction, giving Customers the opportunity to correct or cancel the transaction data.
3. Any transaction successfully carried out by the Customer User and processed by the Bank's system shall be valid, binding, and cannot be canceled, modified, or revoked. All instructions are the full responsibility of the Customers.
4. Customers can utilize the QRIS-QR Payment feature on Mobile Banking services by scanning Static Payment QR Codes and/or Dynamic Payment QR Codes.
5. The fund sources that can be used for QRIS-QR Payment transactions are savings in the form of savings accounts and current accounts in Indonesian Rupiah.
6. To ensure the security of Customers intending to make QRIS-QR Payment transactions, Customers must verify the accuracy of the QRIS Merchant barcode, Merchant name, and transaction amount on the Mobile Banking application screen.
7. Customers enter their PIN to confirm QRIS-QR Payment transactions.
8. The transaction limit for each QRIS-QR Payment transaction adheres to the limits set by Bank Indonesia. Meanwhile, the daily transaction limit for QRIS-QR Payment follows the prevailing regulations of the Bank.

9. Customers conducting QRIS-QR Payment transactions are deemed to have agreed that the Bank has the right to provide transaction data to the receiving party of the QRIS transaction funds.
10. If the payment through QRIS-QR Payment at a Merchant is declared successful but there are complaints/refund requests related to product purchases, Customers can directly contact the QRIS transaction-receiving Merchant.
11. In case of a failed QRIS-QR Payment transaction but the Customer's balance is deducted, Customers can request a refund by contacting Customer Service at Bank Mestika and/or MestikaCall 14083 following the applicable Customer complaint mechanism.
12. The accuracy or error of data recorded on Internet Banking and Mobile Banking is entirely the responsibility of the Customer.
13. If a Financial Transaction is successfully executed by the Bank based on instructions, Customers will receive transaction proof.
14. The Bank reserves the right to not execute transaction instructions from the Customer if the Bank is aware of and has reason to suspect that the transaction is indicative of fraud or criminal activity.

J. OPERATIONAL HOURS

1. Transactions conducted through certain payment systems (SKNBI and RTGS) are subject to the applicable payment system cut-off times.
2. Transactions made after the cut-off time will be processed on the next business day.

K. PROOF

1. In the event that a transaction is carried out by the Customer through e-Mestika and Mestika Mobile, the Customer agrees that the printout from the computer, copy, or form of information storage generated will constitute valid evidence of the Customer’s transactions.
2. By conducting transactions through the Internet Banking and Mobile Banking service, the Customer acknowledges that all instructions and transactions received by the Bank from the Customer will be treated as valid evidence, even if no written documents are created and no sign documents are issued.

L. ADMINISTRATION FEE

1. The Bank will periodically impose administrative fees and/or transaction fees related to the Internet Banking service.
2. The Bank will charge fees for each transaction carried out by the Customer that has been deemed successful.
3. The debiting of administrative fees and transaction fees will be processed automatically by the system.
4. The bank may, at any time, make changes to administrative fees or transaction fees that will be imposed on Customers, provided that it is informed to the Customer in advance. Such changes will be communicated 30 (thirty) working days prior to the effective date of the stated terms and conditions, unless otherwise specified.

M. CUSTOMER RIGHTS

1. To receive security in using products and/or utilizing services in accordance with the provisions of laws and regulations and/or agreements;
2. To choose products and/or services;
3. To receive products and/or services in accordance with the offered terms and conditions and/or as stipulated by laws and regulations;
4. To access the Customer’s data and/or information managed by the Bank;
5. To receive clear, accurate, true, easily accessible and non-misleading information about products and/or services;
6. To have their opinions and complaints heard regarding the products used and/or services utilized;
7. To receive financial education;
8. To be treated or served correctly;

9. To receive advocacy, protection and efforts for complaint handling and dispute resolution in accordance with the provisions of laws and regulations;
10. To receive compensation if the products and/or services received do not comply with the agreement and/or the provisions of laws and regulations;
11. Other rights as stipulated by the provisions of laws and regulations.

Bank Mestika has informed that the rights of the Customer as a Personal Data Subject have been explained in detail in the Privacy Notice available on the Bank Mestika website, https://www.bankmestika.co.id/id/security-privacy.

N. CUSTOMER RESPONSIBILITIES

1. To listen to explanations about products and/or services conveyed through specific marketing methods by the Bank before purchasing the Bank's products and/or services;
2. To read, understand and correctly implement agreements and/or documents regarding the use of products and/or services;
3. To act in good faith when using products and/or services;
4. To provide clear, accurate, true and non-misleading information and/or documents;
5. To make payments in accordance with the agreed-upon value, price, and/or fees for products and/or services with the Bank;
6. To participate in dispute resolution efforts under Consumer Protection regulations in accordance with the provisions of laws and regulations.
7. To report to the Bank if becoming aware of or reasonably suspecting any misuse of the account, credentials, Mobile Token, or any unauthorized transactions.
8. To be responsible for losses resulting from fraud that occurs because the customer voluntarily provides data/codes to another party.
9. To safeguard and not grant access to banking devices, accounts, or applications to any other party.

O. *FORCE MAJEURE*

1. Customers will release the Bank from all legal claims in the event that the Bank is unable to carry out transactions for Customers, whether in part or in whole, due to natural disasters, hazardous situations, armed conflicts, riots, equipment system malfunctions, power outages, telecommunication disruptions, government policies, as well as events or causes beyond the control and/or capability of the Bank.
2. The Bank is not responsible for transaction failures if there is damage to the Internet Banking application caused by Customer errors, omissions, or other reasons such as viruses (trojans, worms, etc.), power interruptions, hardware computer damage and others.

P. CLOSURE OF INDIVIDUAL INTERNET BANKING USAGE

The Internet Banking and Mobile Banking service will terminate if any of the following points are met:

a. The Customer submits a written request for the closure of the Internet Banking and Mobile Banking usage by completing the Internet Banking / Mobile Banking Closure Form provided by the Bank through the nearest bank office.
b. By agreeing to close the Internet Banking service, the system will automatically close the Customer's Mobile Banking service.
c. The Customer closes the account registered as the primary account.
d. The Bank identifies indications of account misuse or fraud by the Customer in relation to legal violations.
e. The Bank fulfils an obligation to terminate access to the Internet Banking and Mobile Banking service due to legal requirements.
f. The Bank discontinues the provision of the Internet Banking service by providing notice to Customers, either verbally or in writing, 30 (thirty) working days before the termination of the provision of such services.

Q. CHANGES OF TERMS AND CONDITIONS

The Bank may at any time make changes, additions, and/or replacements to the Terms and Conditions of Individual Internet Banking and Mobile Banking PT. Bank Mestika Dharma Tbk., with prior notice to Customers through means of communications deemed suitable and appropriate by the Bank, 30 (thirty) working days before the effective date of the said terms and conditions, unless otherwise specified. Any changes to these terms and conditions bind to the Customer.

R. INFORMATION AND COMPLAINTS

Any complaints related to the use of the Internet Banking and Mobile Banking service submitted by Customers can be made through various methods; in person, by phone, in print, and/or electronic mail, as well as through Financial Services Authority (OJK) consumer service. However, this does not include complaints made through media reporting. Customers can submit complaints using a Customer Complaint Form, which should include at least the following information:

a. Customer's name
b. Account number
c. Description of the complaint
d. Name and signature of the officer handling the customer service and complaint resolution.

The Customer may contact MestikaCall at 14083, via email at customer.care@bankmestika.co.id, through the website www.bankmestika.co.id, or by visiting the nearest Bank Mestika branch to obtain information, submit requests, and/or lodge complaints. If the Customer wishes to submit a written complaint, the Customer must provide supporting evidence for such complaint, as may be requested by the Bank.

In case there is no agreement on the resolution of complaints between the User Customer and the Bank, the User Customer may:

a. Submit complaints to the financial sector authority for complaint resolution according to their respective jurisdiction; or
b. File a dispute with an institution or dispute resolution body approved by the financial sector authority or to the court.

The Customer hereby gives consent to Bank Mestika to disclose the Customer's personal information/ data/statements/documents to Bank Indonesia, the Financial Services Authority (Otoritas Jasa Keuangan "OJK"), other relevant authorities in accordance with applicable laws and regulations, including but not limited to third parties such as Notaries, Land Deed Officials (PPAT), and other service providers offering services for and/or on behalf of Bank Mestika.

These terms and conditions may be changed, added, or updated by the Bank from time to time in accordance with the prevailing laws and regulations in the Republic of Indonesia, especially in the field of Banking, including but not limited to regulations issued by Bank Indonesia, the Financial Services Authority, and/or the Bank's internal regulations, as well as other rules and customs applicable at the time and place the actions and approvals are carried out. User Customers are obliged to comply and be bound by such changes, additions, or updates. These terms and conditions are an integral part of the general terms and conditions applicable at the Bank.