BANK MESTIKA

TERMS AND CONDITIONS
CORPORATE INTERNET 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 corporate/business entity account with the Bank.
3. The Bank Customer has registered Corporate Internet Banking User.
4. Corporate Internet Bankingis the utilization of Internet technology used by banks as a platform for Customers to conduct various banking transactions through a web browser application.
5. Mobile Token Corporate, hereinafter referred to as Mobile Token, is a software program within the Mestika Token Corporate application used to authenticate transactions from Bank Mestika's Corporate Internet Banking.
6. Company ID and/or 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 Corporate Internet Banking services.
7. Corporate Admin is an identity created by the system for operating Corporate Internet Banking services by Customers, consisting of Sysadmin 1 and Sysadmin 2 to perform token registration, token approval, token and user lock/unlock.
8. Corporate User is an identity created by the system for operating Corporate Internet Banking services by Customers, consisting of roles such as Maker, Approval, and Releaser responsible for creating, approving, releasing, and rejecting transactions.
9. The Corporate Internet 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 Corporate Internet Banking services.
10. 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.
11. Challenge Number is a series of numbers (consisting of 8 digits) displayed on the confirmation page when Customers are about to perform Corporate Internet Banking service activities. Customers are required to enter it into the Mobile Token to obtain the Response Code, which will be entered into the available response column.
12. Response Code is a sequence of 10 (ten) digits that serves as a one-time secret code generated by the Mobile Token. It is used to authenticate each Financial and Non-Financial Transaction conducted through Corporate Internet Banking.
13. 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.
14. Banking Transactions consist of non-financial transactions and financial transactions.
15. Non-Financial Transactions are information services in the form of transactions that do not affect the account balance.
16. Financial Transactions are services provided by the Bank to Customers in the form of transactions that impact the account balance.

17. 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.
18. The Primary Account is the account in the name of the User Customer that is active and is the first account registered in Corporate Internet Banking service for the debiting of fees in accordance with the Bank's internal policies.
19. The Account List is all the account numbers owned by the Customer, registered and accessible by the Customer.
20. Corporate Internet Banking Application Form is a form that must be filled out by Customers during registration/addition/changes/reactivation/closure of services/other activities on Corporate Internet Banking.
21. The Notifications service sends SMS messages for OTP codes and emails for both successful and unsuccessful transactions conducted by Customers through Corporate Internet Banking.
22. Facilities encompass all the services available within Corporate Internet Banking, which may change at any time in accordance with the bank's internal policies.
23. Maximum Retry refers to a maximum of 3 (three) password attempts by the Customer before being locked by the system.
24. Password Validity Day is the duration of the validity period for the specific password for Customers of Corporate Internet Banking.
25. User Soft Deleted Day is the period for the deletion of a specific User ID for Customers of Corporate Internet Banking by the system if there is no login to Corporate Internet Banking services for a certain period of time.

B. ACCOUNT

1. Accounts that can be registered for Corporate Internet Banking services must be corporate/business entity accounts.
2. The Main Account and other accounts registered in Corporate Internet Banking services are accounts within one Customer Information File (CIF).
3. 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).
4. Information on the guarantee interest rate can be accessed via https://apps.lps.go.id/BankPesertaLPSRate.
5. 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 Corporate Internet Banking service is correct.
2. Misuse of the mobile phone number registered to the Internet 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 Corporate Internet 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 Corporate Internet Banking services are entirely the responsibility of the Customer.

E. REGISTRATION FOR CORPORATE INTERNET BANKINGSERVICE

1. Customers initiate the first stage of Corporate Internet Banking registration through Customer Service.
2. Customers must have a registered email address and mobile phone number at Bank Mestika.
3. Customers are willing to provide information and submit valid documents in accordance with the latest Articles of Association of the Company for photocopying (as part of the Customer's data archive at the Bank) and proof of account holder ownership.
4. Customers will receive notifications via SMS and email containing the password for a successful registration.
5. Complete the second stage of registration by combining the passwords received from SMS and email.
6. Customers can update their customer information by filling out the Customer Identity Form at the nearest bank branch.
7. Customers have read and understood the Terms and Conditions of Corporate Internet Banking.

F. *COMPANY ID, 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 Corporate Internet Banking service at https://corp.bankmestika.co.id/.
2. Password Validity Day is 90 (ninety) calendar days. If after 90 (ninety) calendar days Customers do not change their password, they will be prompted to replace the password during login.
3. The User Soft Deleted Day is 90 (ninety) calendar days. If after 90 (ninety) calendar days Customers do not log in to Corporate Internet Banking service, the system will delete the Corporate User (Maker role, Approval role, and Releaser role) of Customers in Corporate Internet Banking.
4. Used Passwords can be reused after using 3 (three) different passwords.

5. The system will provide notifications to Customers of Corporate Internet Banking when logging into the Corporate Internet Banking system 3 (three) calendar days before Password Validity Day.
6. Corporate Users can initiate a forgot password process on Corporate Internet Banking by entering the Company ID, User ID, and the email registered with the Bank in the following situations:
   a. The Customer forgets their password.
   b. The Customer has reached the Maximum Retry limit of 3 (three) times in a row on the same day.
7. Corporate Admins who forget their password can contact the Bank's Customer Service for assistance.
8. Customers must visit the Customer Service in person to re-register for Corporate Internet Banking if they forget their User ID and/or email address.
9. Customers are required to secure their Company ID, User ID, Password and PIN by:
   a. Not disclosing Company ID, User ID, Password and PIN to others.
   b. Not writing down the Password and PIN on any media, storing them in written form or other storage methods that could be discovered by others.
   c. Promptly delete SMS and email containing the password of Customers of Corporate Internet Banking
   d. Regularly changing the Password.
   e. Advised to Not performing Corporate Internet Banking transactions on publicly used computers and/or accessing the service through free/public internet facilities or Wi-Fi services.
   f. Ensure that the visited website is the official Corporate Internet Banking site as informed by the Bank.
   g. Logging out immediately after completing a transaction(s) using the Corporate Internet Banking service.
11. The confidentiality of the Company ID, User ID, Password and PIN is entirely the responsibility of the Customer.
12. Do not use PIN combinations that are easily known by others.
13. The use of the Company ID, 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 Corporate Internet Banking is an authorization given by the Customer to the Bank to conduct transactions.
14. 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.
15. The Bank is exempt from any legal claims if there is a misuses of the Company ID, User ID, Password and PIN by irresponsible parties because of the Customer’s negligence.

G. CHANGE OF SERVICE FACILITIES OR LIMITS

1. Corporate Internet Banking Customers are allowed to request changes to existing service facilities or transaction limits, and it must be submitted in writing to the Bank at least 30 (thirty) calendar days before the effective date of the change.
2. The Bank has the authority to approve or reject requests for changes to service facilities and/or transaction limits.

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 Corporate 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 specified by the Bank.
4. The Mobile Token cannot be used for other purposes outside of authenticating Financial and Non-Financial transactions specified by the Bank.
5. Customers are required to delete the Mobile Token application stored in their smartphones/devices if they intend to change their mobile phone number and/or use a different smartphone/device.
6. 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. CORPORATE INTERNET BANKING ACCESS

1. Customers can access the Corporate Internet Banking service through the Bank Mestika website at www.bankmestika.co.id.
2. Customers can access the Corporate Internet Banking service by entering the Company ID, User ID and Password correctly.
3. 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.
4. For security purposes, Customers are advised to not access the Internet Banking through free internet service facilities or free Wi-Fi services .
5. Any losses suffered by Customers as a result of using free internet service facilities or free Wi-Fi services as referred to in point 4 above are entirely the responsibility of the Customer.

J. TRANSACTIONS

1. Customers must provide or fill in all required data for each transaction accurately and correctly.
2. In every Financial Transaction, the system will always confirm the data recorded or stated in Corporate Internet Banking, and Customers are given 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. The accuracy or correctness of the data recorded in the Corporate Internet Banking service is entirely the responsibility of the Customer.
5. The Customer will receive a transaction receipt if a financial transaction is successfully carried out by the Bank.
6. 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.

K. 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.

L. PROOF

1. In the event that a transaction is carried out by the Customer through Corporate Internet Banking, 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 Corporate Internet 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.

M. ADMINISTRATION FEE

1. The Bank will periodically impose administrative fees and/or transaction fees related to the Corporate 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.

N. 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.

O. 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.

P. 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.

Q. CLOSURE OF CORPORATE INTERNET BANKINGSERVICE

The Corporate Corporate Internet Bankingservice will terminate if any of the following points are met:

a. The Customer submits a written request for the closure of the Corporate Internet Banking usage by completing the Corporate Internet Banking Closure Form provided by the Bank through the nearest bank branch.
b. The Customer closes the account registered as to the Corporate Internet Banking.
c. The Bank identifies indications of account misuse or fraud by the Customer in relation to legal violations.
d. The Bank fulfills an obligation to terminate access to the Corporate Internet Banking service due to legal requirements.
e. The Bank discontinues the provision of the Corporate 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.

R. CHANGES OF TERMS AND CONDITIONS

The Bank may at any time make changes, additions, and/or replacements to the Terms and Conditions of Online Registration for Corporate Internet 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.

S. INFORMATION AND COMPLAINTS

Any complaints related to the use of the Corporate Internet 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.

*Corporate Internet Banking*In the event that there is no agreement on the resolution of complaints between the Customer and the Bank, the Customer may:

a. Submit the complaint to the financial sector authority for complaint handling within their respective jurisdiction or
b. File a dispute with a dispute resolution institution/body approved by the financial sector authority or with a 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 amended, added to, 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 that apply at the time and place of the action and agreement implementation. Customers are obliged to comply with, be bound by and accept the changes, additions, or updates to these terms and conditions. These terms and conditions are an integral part of the general terms and conditions applicable at the Bank.