

RULES FOR USING OF DANSKE EBANK

Applicable from 25 November 2017

GENERAL PROVISIONS

1. The definitions used in these Rules for using of Danske eBank (the 'Rules') shall be interpreted using the definitions provided in the Standard Terms and Conditions of Danske eBank Agreement. These Rules are an integral part of the Standard Terms and Conditions of Danske eBank.
2. Information on the use of Danske eBank and Danske mBank shall be provided on www.danskebank.lt and by telephone on short number 1636 (for customers abroad: +370 5 215 6666) on working days from 8.00 to 17.00.
3. Prior starting to use Danske eBank for the first time, the User should read the information provided in Danske eBank Help section on www.danskebank.lt/ebankas.
4. In the event of communication or software failures as well as during periods of maintenance of Danske eBank and/or Danske mBank, the Bank shall service the Customers at its customer service units during their working hours. The Users shall be informed about estimated maintenance periods and failure correction periods on log in website of Danske eBank <https://e.danskebank.lt> and/or the Bank's website www.danskebank.lt.
5. The Bank shall be entitled to change functionalities of Danske eBank and Danske mBank unilaterally without amending these Rules.

DANSKE EBANK USERS

6. The Customer may specify one or more Users that will manage the Customer's accounts by Danske eBank and Danske mBank.
7. The User specified by the Customer shall be a natural person authorised by the Customer to manage its accounts and take other actions in Danske eBank. The right of management shall be assigned to the User automatically, without a special request, with respect to accounts in other currencies opened under the existing account number.
8. The User rights shall be set in the agreements and requests for the use of Danske eBank and Danske mBank signed by the Customer.
9. The Customer may assign to the User the following management rights:
 - 9.1. Entering transactions;
 - 9.2. Approving transactions with Signature level A (the transaction is submitted to the Bank for processing upon approval by at least one User having the right of Signature level A);
 - 9.3. Approving transactions with Signature level E (the transaction is submitted to the Users with the right of Signature level A upon approval by at least one User having the right of Signature level E);
 - 9.4. Change the services received by the User/Users through Danske eBank and Danske mBank;
 - 9.5. Establish that each transaction shall be approved by all the Users of Signature level A and/or Signature level E;
 - 9.6. Establish that Users with the right of Signature level E may submit transactions up to a certain amount to the Bank for processing without approval of the Users with the right of Signature level A.
 - 9.7. Subject to the Bank's consent, establish special signature groups to Users according to the Customer's needs.
10. The Customer may assign the following account management rights to the User:
 - 10.1. **View Only** - viewing account balance, statement of account and other information;

- 10.2. **Credit Only** - making transfers to the account;
- 10.3. **Debit Only** - making transfers from the account;
- 10.4. **Credit and Debit** - making transfers to/from the account.
11. The Customer may set the following transactions limits to each account managed by the User:
 - 11.1. **Per transaction** - the largest amount of money for which the User may approve an transaction from the specified account;
 - 11.2. **Per day** - the largest amount of money for which the User may approve transactions from the specified account per day;
 - 11.3. **Per month** - the largest amount of money for which the User may approve transactions from the specified account per calendar month;
12. The limits and rights shall be specified in the agreement concluded with the Bank and in the Menu of Danske eBank: **Information and Settings -> Session information, section Account Limits** (additionally, the Users may view the amounts used in this section).
13. Apart from performing transactions, concluding agreements and other transactions on the Customer's behalf, the Users of Danske eBank may also view information about deposit, credit, leasing and other agreements concluded on the Customer's behalf and services to the Customer and, if the Bank makes such a possibility, log-in to third-party portals where they may take, on the Customer's behalf, actions permitted by third parties (order services, conclude agreements etc.). As the Users of Danske eBank are assigned and the scope of their authorisations is set by the Customer, the Bank shall not be liable for the information on the Customer's transactions on Danske eBank and Danske mBank disclosed to the Users and the User's actions taken on behalf of the Customer in Danske eBank, Danske mBank and third-party systems.

USER IDENTIFICATION MEANS

14. The Bank shall identify the User according to the User ID. The Bank shall provide the User with the following identification means:
 - 14.1. **User ID** - a User code which shall not be changed and shall only be used for logging in to Danske eBank and Danske mBank;
 - 14.2. **Password generator** is a device that generates unique one-off passwords to be used when logging in to Danske eBank and Danske mBank and for the confirming of transactions:
 - 14.2.1. An explanation of how to use the password generator is published on the Bank's website www.danskebank.lt.
 - 14.2.2. The password generator is protected by a PIN code ('PIN'). Upon turning on the password generator for the first time, the User has to create a 4-digit PIN that will be used each time when using the password generator.
 - 14.2.3. If the User enters a wrong PIN three times, the generator will be blocked. The User can de-block it at the Bank (upon presentation of a personal ID document and the generator).
 - 14.3. A qualified electronic signature issued by a certification services provider meeting the requirements set by a competent institution of the Republic of Lithuania, acceptable to the Bank, may be used for the identification of the User.
15. Should the User lose/damage the Identification mean, the User shall visit the Bank's customer service unit or call the Bank on 1636 (for customers abroad: +370 5 215 6666).

16. The Customer shall recognise and consider to be signed any instructions and notices sent by the Customer and the User, any agreements concluded and any other actions taken through Danske eBank and Danske mBank if they have been approved by correct Identification means. The parties explicitly agree that an electronic signature generated by the User's Identification means has the same legal power as a signature in written documents and shall be admissible as evidence in court.

ENTERING, CONFIRMING AND EXECUTING TRANSACTIONS

17. Transactions (money transfers, execution of agreements and other instructions) in Danske eBank and Danske mBank shall be initiated by selecting the relevant item on the Menu and entering the requisite information.

18. In order to submit a transaction to the Bank, the User shall click on **Enter** (in Danske mBank - on **Next**) and approved the transaction by Identification means.

19. The transaction will not be submitted to the Bank for execution if the User has clicked on **Defer Approval**. The transaction will be seen on the list of transactions not signed in the Menu (**Daily Services -> Order Lists -> Not Confirmed**). The User may enter a several transactions in Danske eBank and approve them at the same time, upon opening the list of transactions not approved.

20. The transactions entered in Danske eBank and Danske mBank are grouped into four lists (**Daily Services -> Order Lists**):

20.1. **Not Confirmed** - transactions that have been entered but not approved by the User;

20.2. **Confirmed** - transactions approved by the User but not yet executed by the Bank or not yet approved by other Users of the Customer;

20.3. **Rejected** - transactions approved by the User in which errors have been found, or funds in the Customer's accounts were insufficient for the execution of the transaction and/or debiting of the service fees;

20.4. **Executed** - transactions approved by the User and executed by the Bank. Information on payments made is also provided in the statement of account on Danske eBank in Menu path **Daily Services -> Statement**.

21. Should any questions about execution of transactions on Danske eBank arise, additional information can be obtained by clicking on **Help** (top right corner of the window). Here the conditions of execution of transactions are explained (terms, limitation on amounts etc.) which may or may not differ from the conditions in the Price List but which are relevant to specific transactions.

22. If the User instructs the Bank to make a transfer from the Customer's account, the User must ensure that the transaction is entered correctly and that there are sufficient funds in the Customers account for the execution of the transfer and the payment of the Bank's fees.

23. The User shall, at least once in a month, using the Menu path **Daily Services -> Order Lists**:

23.1. Check transactions on Danske eBank and Danske mBank submitted to the Bank after the last check;

23.2. Remove any transactions that have not been executed and are unnecessary;

23.3. Immediately inform the Bank about any suspicious transactions which have not been submitted to the Bank by the User but which are indicated on Danske eBank or Danske mBank as the transactions made by the User, by calling on 1636 (for customers abroad: +370 5 215 6666) or by visiting the Bank's customer service unit. In addition, the User must block the log-in to Danske eBank if possible (Menu path **Information and Settings -> Session Information**).

SAFE USE OF DANSKE EBANK

24. The User shall work with Danske eBank on a computer with Internet connection and a browser which enables a log-in to Danske eBank (the browser version is checked during log-in, therefore, if the version is outdated, the User may receive warning messages or logging-in to Danske eBank may be banned). Danske mBank can be used by Customers using Android and iOS operating systems in their mobile phones.

25. The User who uses Danske eBank and Danske mBank shall make sure that the software used will not damage, modify or otherwise disrupt the information and computer systems of the Bank and will not cause damage to the Bank, other Customers of the Bank or third parties, and that no other actions not authorised by the Bank will be taken.

26. The User shall maintain secrecy of the Identification means provided, shall not transfer them to anybody and shall not make copies thereof.


27. Should the User lose the Identification means or suspect that they have become known to third parties, the User shall immediately block the log-in to Danske eBank if possible (Menu path **Information and Settings -> Session Information**), and immediately call the Bank on 1636 (for customers abroad: +370 5 215 6666) or visit the Bank's customer service unit.

28. Upon proper reporting the loss or disclosure of the Identification means by the User, the Bank shall block log-in to the system and the User will be able to log in only after the Customer submits a request to issue new Identification means at the Bank.

29. Upon log-in to Danske eBank, the User must make sure that it is the right website:

29.1. the beginning of the address must be [https://e.danskebank.lt/...](https://e.danskebank.lt/);

29.2. there must be a lock pictogram in the browser window

 (GlobalSign certificate). If no such pictogram is seen, the User shall discontinue work and notify the Bank by calling 1636 (for customers abroad: +370 5 215 6666).

30. If the User has not taken any action in Danske eBank during 20 minutes, the User has to log in repeatedly in order to continue working.

31. If the User has not taken any action in Danske mBank during 10 minutes, the User has to log in repeatedly in order to continue working.

32. After finishing work in Danske eBank or Danske mBank, the User has to log off by clicking 'Exit' (in the top right corner; for Danske mBank - in the middle of the menu circle) and to close the browser window (for Danske eBank).

33. The User shall be responsible for the security of the computer or a smart phone on which he/she logs in to Danske eBank or Danske mBank, e. g. by using anti-virus programs etc., and for any consequences arising from a failure to ensure appropriate protection of the Customer's/User's computer systems or other systems.

34. The Bank shall be entitled to block the User's log-in to Danske eBank and Danske mBank in the following cases:

34.1. The User enters a wrong Password from the password generator three times;

34.2. The User has not logged in to Danske eBank or Danske mBank for four hundred days in succession;

34.3. The Customer has submitted a request to the Bank to stop the use of Danske eBank by the User;

34.4. For other reasons specified in the General Conditions of the Bank and agreements concluded with the Customer.

35. In order to cancel the blocking of Danske eBank and/or Danske mBank and to be able to log in to Danske eBank and Danske mBank again, the Customer has to visit the Bank's

customer service unit or call 1636 (for customers abroad: +370 5 215 6666).

36. The Bank warns the Customer and the Users that they may receive emails or calls from individuals pretending that they are employees of the Bank or officers and requesting to provide passwords for the log-in to Danske eBank or Danske mBank or to log-in, for an allegedly serious reason, to Danske eBank or Danske mBank and enter the details of the Identification means. The Customer/User must keep the log-in data provided to him/her secret, not submit to the provocation, and inform the Bank about such attempts immediately by calling 1636 (for customers abroad: +370 5 215 6666) or by visiting the nearest customer service unit of the Bank.

37. Prior to starting the use of Danske eBank or Danske mBank for the first time, and each time when the Bank requests, the User shall familiarise himself/herself with the advice on safe use of Danske eBank published on the Bank's website www.danskebank.lt/saugusbankas, and shall take all actions recommended therein.

38. In order to ensure security of the Customer's funds, the Bank shall have the right (but not the duty) to send SMS to the mobile phone number provided by the Customer and the User, informing about the signed transactions that exceed the limit set by the Bank (the User may refuse from such SMS by calling the Bank on 1636 (for customers abroad: +370 5 215 6666), as well as other SMS informing the User about potentially suspicious transactions, recent attempts to fraudulently obtain log-in data from the Users etc. The Bank shall have the right to stop sending such SMS without notifying the Customer and the User.

FUNCTIONS OF DANSKE MBANK

39. Danske mBank is a component of Danske eBank that enables the performance of transactions in Danske eBank through an application for mobile phones. Only part of the functions of Danske eBank are accessible through Danske mBank, e. g. overview of accounts/cards, statement of account, transaction details, payment orders between own accounts in the Bank, EU payment order, currency exchange, lists of payees, domestic payment templates, notices etc.