

## Rules for Using Danske eBank

### Introduction

1. The definitions used in these Rules shall be understood as the ones used in the General Provisions of the Bank Account Agreement.
2. Danske eBank User must fulfil the obligations laid down in the Special Provisions of the Bank Account Agreement (hereinafter - "Agreement") as well as in these Rules.
3. The Bank retains a right to unilaterally change these Rules and undertakes to inform the Client about amendments to the Rules through Danske eBank notifications and on the Bank's website <http://www.danskebankas.lt/en> no later than 14 days prior to the day on which the amendments come into effect.
4. Information about using Danske eBank is available on the Bank's website <http://www.danskebankas.lt/en> or by phone, short number in Lithuania 1636 (from abroad: +370 5 215 6666) every work day from 8:00 to 19:00.
5. User is recommended to view the introductory course available on the Bank's website <http://www.danskebankas.lt/ebankas-duk> prior to using Danske eBank for the first time.
6. The User must use a computer with internet connection and a browser that meets the W3C standards (Microsoft Internet Explorer 5.5, Mozilla Firefox 1.0 or higher versions) for work with Danske eBank.
7. When using Danske eBank, User must ensure that the software will not damage, modify or otherwise interfere with the Bank's information and computer system, that no damage will be done to the Bank, other Bank's clients or third parties, and no other actions unauthorized by the Bank will be carried out.

### Danske eBank Users

8. When entering into a Danske eBank Agreement, Client can indicate one or several Users who will manage the Client's accounts via Danske eBank.
9. The User, specified in the Client's Agreement, is a natural person who has been entrusted by the Client with the management of his accounts under the terms laid down in the Agreement.
10. User's rights are established by the agreements, signed by the Client, as well as the applications for using Danske eBank.
11. At the time of registering a User or by submitting a separate request at a later point in time, the Client may establish the following transaction management rights:
  - 11.1. enter transactions;
  - 11.2. authorize transactions by first signature (the signature of at least one User having a first signature right is sufficient for the transaction to be submitted to the Bank for execution);
  - 11.3. authorize transactions by second signature (the signature of at least one User having a second signature right is sufficient for the transaction to be submitted to the Users having the first signature right);
  - 11.4. change terms of the Agreement applicable to themselves and other Users;
  - 11.5. make a setting that every transaction must be authorized by all first and/or second signature Users;
  - 11.6. make a setting that the Users having a second signature right may submit transactions up to a certain amount to the Bank for execution without the authorization of the Users having a first signature right.
12. At the time of registering a User, Client may establish the following transaction management rights:
  - 12.1. view only - to view account balance, statement and other information;

- 12.2. credit only – to make credit transactions only;
  - 12.3. debit only – to make debit transactions only;
  - 12.4. credit or debit – to make transfers to and from the account.
13. When registering a User, Client may set the following limits (LTL) for entering transactions for each account managed by the User:
- 13.1. per transaction – maximum amount of money, within the limits of which a User may enter one transaction from the indicated account;
  - 13.2. per day – maximum amount of money, within the limits of which a User may enter transactions per day from the indicated account;
  - 13.3. per month – maximum amount of money, within the limits of which a User may enter transactions per one calendar month from the indicated account;
14. Users using password cards are subject to obligatory limits for the amount of authorized transactions - 400 LTL per day and 15000 LTL per month. The limits do not apply to money transfers between own accounts, currency exchange transactions, deposit or direct debit agreements, facility and other service payments.
15. The limits and rights are provided in the Agreement and in the Danske eBank menu bar **Information -> Session Information** (in addition, Users can also see the remaining unused limits on this menu bar).

### Means of User Identification

16. The Bank identifies a User according to the User ID and User password. The Bank issues the following Identification means for the User:
- 16.1. **User ID** – a digital code of the User, which remains unchanged. It is specified in the Agreement. It is used only to access Danske eBank.
  - 16.2. **Initial User password** – a digital password provided in an envelop, which is delivered upon signing of the Agreement. User uses it when accessing Danske eBank for the first time and must change it to a User password.
  - 16.3. **User password** – a password created by the User, used for every access to Danske eBank:
    - 16.3.1. User must create a password consisting of 6 or more letters and numbers. Spaces, Lithuanian alphabet letters or special symbols are not recommended. The password must be a meaningless sequence of numbers or letters. A telephone number, person's name or other information related with the User must not be used for creating a password;
    - 16.3.2. for safety reasons, User password must be changed on a regular basis; therefore, Danske eBank will suggest changing it 60 days from the last change of the password. User may change the password in Danske eBank menu bar **Settings -> Change Logon Password**.
  - 16.4. **Password card** – a plastic card with 24 passwords, used by User for accessing Danske eBank and for signing transactions. The password card must be kept as safe as a password: it cannot be copied, disclosed to others, etc.
    - 16.4.1. where passwords on the card have letters, there is a dot or a dash inside a zero;
    - 16.4.2. the sequence of numbers at the bottom of the card marked with a hash mark (#) is the card number.
  - 16.5. **Password generator** – a device that meets the highest safety requirements, which generates unique one-off passwords that User uses for accessing Danske eBank and for signing transactions:
    - 16.5.1. Instructions for using a password generator are available on the Bank's website <http://www.danskebankas.lt/ebankas-digipass> a Bank employee may also explain how to use it.

- 16.5.2. Password generator has a protection password (hereinafter - PIN). Upon turning on a password generator for the first time, User must create a 4 digit PIN, which will be used every time when a password generator is turned on.
- 16.5.3. Generator is blocked following 3 incorrect attempts to enter the generator's PIN. In order to unblock the generator, the User must come to a Bank branch (and have a personal identification document as well as the generator).

16.6. Users of Clients (legal persons) are issued only password generators.

- 17. Where User forgets User password or Identification means are lost/damaged, he must turn to the Bank's customer service branch or call the Bank at 1636 (from abroad: +370 5 215 6666).
- 18. Client recognizes and considers signed all notifications, orders, concluded agreements and other actions carried out via Danske eBank by the User, where they are authorized by correct Identification means.

### Entering, authorizing and Executing Transactions

- 19. Transactions (money transfer, conclusion of agreements and other orders) via Danske eBank are prepared by choosing a respective menu item and filling in the necessary information.
- 20. In order to submit a prepared transaction to the Bank for execution, User must sign it by clicking on the button **Enter and Sign** and by entering a password from the password card or password generator.
- 21. Transaction will not be submitted to the Bank for execution if a User clicks on the button **Enter**. This transaction will appear on the list of unauthorized transactions (menu bar **Transactions -> Transaction Lists -> Not Signed**). User may enter several transactions and sign all of them at once by opening the list of unauthorized transactions.
- 22. Transactions entered by a User via Danske eBank are divided into four lists (menu bar **Transactions -> Transaction Lists**):
  - 22.1. **Not Signed** - entered transactions that have not been authorized by User's signature.
  - 22.2. **Signed** - transactions authorized by User's signature but yet unexecuted by the Bank or transactions that are not authorized by other Client's Users.
  - 22.3. **Failed** - transactions authorized by User's signature, during the execution of which mistakes were discovered or the funds in the Client's account were insufficient for the execution of the transaction and/or for covering the fees for the Bank's services.
  - 22.4. **Executed** - transactions authorized by the User's signature and executed by the Bank. Information about the executed payments is additionally available in the account statement on the menu bar **Accounts -> Statement**.
- 23. In case of questions about the execution of transactions in Danske eBank system, additional information is available by clicking on the button **Help** (top right corner). Transaction execution terms (dates, amount limits, etc.), which differ from the terms provided in the Bank's service and transaction charges or do not differ but are significant for a concrete transaction, are available in this section.
- 24. Where User orders for the Bank to execute a transfer from the Client's account, he must ensure that the transaction is entered correctly and that the Client's account has sufficient funds for the execution of the transfer as well as for the fees payable for a respective Bank service.
- 25. At least once a month, in the menu bar **Transactions -> Transaction Lists**, User must:
  - 25.1. review Danske eBank transactions submitted to the Bank after the last review;
  - 25.2. remove irrelevant unexecuted transactions;
  - 25.3. inform the Bank immediately about suspicious transactions, which the User had not submitted to the Bank but which are listed in Danske eBank as performed namely by

the User, by calling 1636 (from abroad: +370 5 215 6666) or by arriving to the Bank's Customer Service Branch. In addition, where a possibility exists, the User must block access to Danske eBank (menu bar **Information -> Session Information -> Disable User**).

26. Danske eBank transaction lists provide transactions of the last 400 days. As far as a report of older transactions is concerned:

26.1. Danske eBank User may order it via Danske eBank notification;

26.2. Client can order it at the Bank's Customer Service Branch.

### Safe Danske eBank Use

27. User must ensure the secrecy of the entrusted Identification means and must not hand them over to anybody or make copies thereof.


27.1. Where User loses the means of Identification or a suspicion arises that the User's Identification means may be known by third parties, the User undertakes to immediately block access to Danske eBank (menu bar **Information -> Session Information -> Disable User**), where such a possibility exists, and inform the Bank about it immediately by calling 1636 (from abroad: +370 5 215 6666) or by arriving to the Bank's Customer Service Branch.

27.2. User and Client shall be liable for the loss incurred in relation with the loss or disclosure of Identification means until a notification to the Bank in one of the following ways;

27.3. Where User properly informs about the loss or disclosure of Identification means, the Bank shall block the User's access and the User will be able to re-access the system only after the Client arrives to the Bank and submits a written request for the issue of new Identification means.

28. After accessing Danske eBank, User must ensure that it is the right website:

28.1. address must begin with [https://ebankas.danskebankas.lt/...](https://ebankas.danskebankas.lt/)

28.2. the browser must show a pictogram of a lock  (sign of Verisign certification). In the absence of this pictogram, the User cannot continue working and must inform the Bank by calling 1636 (from abroad: +370 5 215 6666).

29. Where a User is idle in **Danske eBank** for 10 minutes, he will have to re-enter the User password in order to continue; where a User is idle for 20 minutes, he will have to re-access the system by entering the User password and the code from a Password card or Password generator in order to continue.

30. After finishing working in **Danske eBank**, the User must log off the system by clicking on the button **Exit** (top left corner) and close the browser window.

31. User must ensure the safety of the computer that is used to access **Danske eBank**; for instance, use anti-virus software and other safety measures. User bears the responsibility for all the consequences, arising from insufficient protection of the Client / User computer or other systems.

32. The Bank temporarily blocks User access to Danske eBank:

32.1. where a User enters incorrect User password 5 times;

32.2. where a User enters incorrect Password from a Password card or Password generator 3 times;

32.3. where a Client submits a written request to the Bank to suspend User's access to Danske eBank.

33. In order for the temporary blockage, specified under points 32.1. and 32.2. of these Rules, to be lifted and for the User to regain a possibility to access Danske eBank, User must address the Bank's Customer Service Branch or call 1636 (from abroad: +370 5 215 6666).

34. User may receive letters or calls from persons who pretend to be the Bank employees or other officials and who ask to give out the passwords for accessing Danske eBank or who, due to allegedly important reasons, may try to access Danske eBank and enter all or most of the passwords from the card passwords in a form in Danske eBank. Even in such cases User must keep the data for accessing Danske eBank in secret, must not respond to provocations and must immediately inform the Bank about the attempts to swindle them out of access data by calling 1636 (from abroad: +370 5 215 6666) or by arriving to the Bank's Customer Service Branch.
35. Before using Danske eBank for the first time and in response to each request from the Bank, User undertakes to get acquainted with the recommendations for safe use of Danske eBank, available on the website <http://www.danskebankas.lt/ebankas-safe>, and follow the recommended measures as closely as possible.
-