

GENERAL TERMS FOR USING THE WEB BANKING AND/OR MOBILE BANKING SERVICE/S

I. SUBJECT OF THE SERVICES

1. These terms apply for Silk Road Bank AD Skopje (hereinafter "the Bank") and the Client – a legal or physical entity depending on who applies for using the Web Banking Service and/or Mobile Banking.

2. The Web Banking Service and/or Mobile Banking may be used in the following two ways, depending on the Client's needs:

2.1. Passive Web Banking and/or Mobile Banking – the Client has access to the following information:

- a. viewing the balances of the account
- b. monitoring of the account's activity
- c. information on the Bank's FX rates
- d. change of the password for accessing the system
- e. reading information

2.2. Active Web Banking and/or Mobile Banking – the Client has the same characteristics as the Passive Web Banking and/or Mobile Banking Client, but also has access to electronically initiate and authorize any of the following transactions:

- a. external payments in MKD
- b. internal payments in MKD
- c. creation of beneficiary templates
- d. pending authorization

2.3 The Bank has right to enhance the services of active web banking, and the client is consent for these changes to be adequate informed

3. In order for the Client to use the Web Banking and/or Mobile Banking Service/s they must possess at least one transactional account.

4. The minimal technical requirements for using the "Web Banking Service" is having access to the Internet and using the web browser-Microsoft Edge, Mozilla Firefox, and Google Chrome. The minimal technical requirements for using the "Mobile Banking Service" is having access to the Internet from Smartphone and download the application SilkRoad m-Bank from Google Play Store (for Android) or APP Store (for iOS) or through the official web page of the Bank www.silkroadbank.com.mk.

5. The Bank has the right to place limitations on the performing of the Web Banking and/or Mobile Banking Service operations due to the requirements stipulated by Law, and/or due to maintenance of the necessary security information in its system.

II. ACTIVITY AND ACCESS

6. For using the Service/s:

6.1. The Client submits the previously filled in application for using the Web Banking and/or Mobile Banking Service/s to some of the

Branches of the Bank. In the application the Client provides the accounts which shall be available through the Web Banking and/or Mobile Banking Service/s, as well as their own rights for performing transactions in cases when the Active Service/s is chosen.

6.2. The Client shall sign a contract for using the Web Banking and/or Mobile Banking Service.

7. The contractual relations between the Bank and the Client shall be regulated by the contract for the Web Banking and/or Mobile Banking Service/s, the General Terms and Tariff of the Bank of which are available on the Bank's official web-site www.silkroadbank.com.mk.

8. The Client – individual may start using the "Web Banking" and/or "Mobile Banking Service/s" as of the date of signing the contract and application.

The client – legal entity may start using the "Web Banking" and/or "Mobile Banking Service/s" as of the date of signing the contract, through obtaining digital certificate and/or Username and password, after prior signing the contract and application.

9. The Bank shall register the Client who uses the "Web Banking" and/or "Mobile Banking Service" into the system in accordance with the internal regulations and procedures. The client – individual shall login by using Username and Activation code received first part on the clients' e-mail address, and the second part of the activation code shall be received by SMS. On the other hand, the client – legal entity shall obtain digital certificate and/or Username and password.

10. If the Client applies for using the Active Web Banking and/or Mobile Banking Service/s, which understands initiation and authorization of transactions electronically, they should choose this particular option on the application form for which the Client is charged with a certain fee determined by the valid tariff.

11. The Client shall be granted access to the Web Banking and/or Mobile Banking Service/s within 2 (two) working days from the date of submitting the application. Access to the web-site is provided through the official web-site of the Bank www.silkroadbank.com.mk

III. SECURITY

12. The Bank identifies the Client by their username and password.

12.1. The password represents a secret code which when combined with the username allows the Bank to identify the Client and grant them or their authorized representative access to the system. The Client has the right to alter their

password at any time and upon request by the system.

13. If the Client - individual chooses to use the Active "Web Banking" and/or "Mobile Banking" Service/s, for confirmation of the inputted transaction should input OTP code (one-time password), and for "Mobile Banking" Service besides the OTP code, there is possibility the transaction to be confirmed with FaceID or FingerPrint (in accordance with the operating system of the mobile device).

If the client – legal entity chooses to use the Passive "Web Banking Service" and/or "Mobile Banking" Service, it is required usage of Username and password, and if the client chooses the Active "Web Banking Service" and/or "Mobile Banking" Service it is mandatory usage of Digital Certificate or Username and password.

Received passwords, codes and digital certificate are used for identification and greater security when accessing the system. As well as for confirmation for further usage and performance of the banking operations by the Bank. The performed transaction with such verified identification is irreversible.

14. The username and password - OTP code for clients - individuals and digital certificate for clients – legal entities are electronic identification of the Client.

15. The Client is obliged to keep safe and exclusively to themselves all the devices and data for electronic identification.

16. The Bank shall not bear any responsibility for the consequences which may occur in case the devices and data for electronic identification of the Client became disposed to unauthorized persons.

17. In case the password or the digital certificate or mobile device for the OTP service are lost or they fall into the possession unauthorized/illegal users, the Client has to inform the Bank immediately on the telephone number: +389 2 3289 440 or the next working day they should visit the Bank and fill in an application.

18. The Bank has the right to block the access to the system to those Clients and persons authorized by them whose actions are violating the Bank's provisions or represent a threat to the security of the system

19. The Client (legal entity) shall have the right to authorize third parties to gain access to the Service/s, for which the Client has to fill in applications and choose the option "authorization". The applications have to be provided with information on all the relevant data concerning the persons who shall have access to the Service/s, as well as the regulations for

reviewing the accounts and performing transactions with certain limitations. The application has to be verified and signed by an authorized person from the company, as well as from the other authorized persons (authorizers/initiators).

20. The service/s Web Banking and/or Mobile Banking is/are used personally and exclusively by the Client and third parties do not have the right to access the service/s. For Clients with limited working capacity (minors, disabled persons, etc) the service/s is/are used exclusively by the legal representative/guardian of the Client with limited working capacity.

21. The Bank shall be obliged to provide each person (legal entities: authorizer/initiator) with a username and password for accessing the Service/s within 2 (two) working days.

22. In case the Client (legal entity) wishes to alter/ terminate/ add certain access of the persons (initiator/authorizer) to the Service/s, they need to fill in an application where they have chosen the option alteration of personal data/authorization/deactivating registration.

23. The Client (legal entity) guarantees that the users authorizers/initiators who possess devices and data for electronic identification shall comply with the terms and provisions defined by the Bank.

24. The Client (legal entity) assumes full responsibility for any act or oversight by the user's authorizers/initiators as a result of violation of the terms and provisions defined by the Bank.

25. The Client (physical person) assumes full responsibility for any act or oversight as a result of violation of the terms and provisions defined by the Bank.

26. The Client shall be responsible and obliged for all the activities which shall be taken on their account and on their behalf in the system.

IV. RESPONSIBILITIES

27. The Bank shall not be responsible for the consequences which may result from the illegal and/or incompetent use of the Web Banking and/or Mobile Banking Service/s.

28. The Bank shall not be responsible for actions performed with unauthorized use by third parties who penetrated the system using the devices and information for electronic identification for Web Banking and/or Mobile Banking Service/s.

29. The Bank shall not be responsible for overdue or unsuccessful transactions as a result of incorrect or false data provided by the Client, as a result of technical problems in case of force majeure, or a case of negligence or incorrect performance by the Bank.

30. Any information used by the Client to initiate any transaction whatsoever is considered correct. The Bank shall not be obliged to review

this information and/or confirm its validity.

31. The Bank shall not assume responsibility for overdue or unrealized transactions performed by third parties in the following circumstances as well:

31.1. If there are no sufficient funds on the Client's account for the performance of the transaction or there are not enough funds to cover the banking fee.

31.2. If the account is closed or blocked from some reason;

31.3. In case of unavailability of the official web-site of the Bank due to: technical, telecommunication problems, or severance of the Internet access.

31.4. If the Client is not in compliance with the provisions of the Bank relative to the proper and duly deliverance of an order in accordance with the payment system in the Republic of Macedonia.

V. FEES AND COMMISSIONS

32. The Client – Individual for using the Passive “Web Banking” and/or “Mobile Banking” Service shall not be charged by the Bank, and for using Passive “Mobile Banking” the client shall be charged one-time fee for using the mobile application.

33. The Client - individual shall pay a one-time fee to the Bank for initiating the Active “Web Banking” and/ or “Mobile Banking” Service/s (Silk m-Token) as well as monthly fee for using the services in accordance with the valid Tariff of the Bank.

The Client - legal entity for using the Passive “Web Banking and Mobile Banking” services shall pay a monthly fee for the services and one-time fee for using the “Mobile Banking” application. For using the Active Web Banking and Mobile Banking Service the client shall pay monthly fee for the services and one-time fee for using the mobile application, as well as fee for issuance of Digital Certificate (for client – legal entity) stated in the Tariff of the Bank.

The fee shall be charged from the clients' account stated in the application or personally at the Bank's counters.

34. In case of lack of funds on the Client's account or a closed account for covering the expenses (point 33), the Bank shall have the right to conduct a payment from other accounts in the Bank in accordance with the provisions stipulated by the Bank

35. For all the transactions carried out through the Active Web Banking and/or Mobile Banking Service/s the Bank charges the Client's account which is designated as the account for conducting operations connected with debts, fees, and commissions determined by the Bank's tariff.

36. In case of insufficient availability of the Client's account for paying the expenses for conducting the transaction, the same shall be cancelled.

37. The Bank retains the right to alter the tariff and is obliged to inform the Client of such decision through the Branches of the Bank, the official web-site, etc. The Client shall agree with such alterations.

VI. TERMINATION OF THE USE OF THE SERVICE/S

38. The contractual relations between the Bank and the Client, established with the contract for Web Banking and/or Mobile Banking Service and with the signing of the provisions from the General Terms of the application for using the Service may be terminated unilaterally by any of the contractual parties with a one month written notification. The termination of the contract shall not exempt the contractual parties from the obligations assumed before the termination

39. The Bank shall have the right to terminate the Web Banking and/or Mobile Banking Service/s in the following cases:

39.1. If the Client does not comply with the terms determined with the General Terms

39.2. Closing of all the Client's accounts in the Bank

39.3. Death of the Client -physical person

39.4. In case of going into receivership, liquidation, transformation or termination by the authorized bodies of either of the parties.

39.5 risk assessment from incompliance of the client performance with the current legislative in the country.

40. The General Terms shall stay into force until the termination of the obligations of both parties.

VII. ADDITIONAL PROVISIONS

41. The Bank shall have the right to alter the General Terms at any time and is obliged to inform the Client through notifications placed in an appropriate location, sent by e-mail, or communicated using any other means that the Bank considers appropriate. If the Client continues to use the Web Banking and/or Mobile Service/s after they were notified of the alterations of the General Terms, it shall be considered that the Client accepts the alterations.

42. By signing the contract for using the Web Banking and/or Mobile Service/s the Client states that they have voluntarily provided their personal data and the data of the users (initiators/authorizers) and makes a statement with which they authorize the Bank to use and process their personal data and the personal data of the users (initiator/authorizer), in accordance with the law on personal data protection.

