2.2. Terms and Conditions of Remote Account Management Services

Special Terms

User means the Customer and/or another individual authorised by the Customer to use the Remote Account Management Services to a certain extent.

Remote Account Management Services mean account management using the Internet Bank or electronic mail.

Internet Bank means a remote account management system in the online mode, which is available on the Bank's page https://ibank.privatbank.lv.

Access Parameters mean combinations of digits and/or Latin alphabet characters (username and login password) used for Customer Authentication in Privat24.

Authorisation Tools mean special technical tools or parameters that are used by the User for confirmation of Transaction Documents/Notifications and for sending thereof to the Bank, and that ensure the Customer Authentication and authenticity of such Transaction Documents/Notifications. Authorisation Tools are as follows:

- **Digipass Device** means an electronic device with a PIN or without it – depending on the device model, which generates numerical codes. Digipass Device is envisaged for Customer authentication in Internet Bank, for sending instructions/payment orders of the Customer to the Bank by mail or by e-mail, for Customer authentication via phone or online chat. The limit of the one operation is not specified;

  PrivatSecure means a mobile application of the Bank with a PIN code, which generates numerical codes (envisaged for smartphones running Android OS, version 2.3 and above, as well as for smartphones running iOS v8 or above). PrivatSecure is **available for download at Google Play**: https://play.google.com/store/apps/details?id=lv.privatbank.secure.privatsecure or **on the App Store**: https://itunes.apple.com/us/app/privatsecure/id1265155138?mt=8.
  In order to use PrivatSecure, the Bank provides the Customer with a serial number and an activation code. PrivatSecure is envisaged for Customer authentication in Internet Bank, for sending instructions by mail or by e-mail, for Customer authentication via phone or in Online Chat. The limit of the one operation is not specified;
- **SMS Password** means a one-use digit code sent to the User to their specified mobile phone number as a text message for use in Internet Bank, for Customer authentication via phone or in Online Chat.

Authentication means a procedure allowing the Bank to verify the identity of a Customer.

General provisions:

2.2.1. Terms and Conditions of Remote Account Management Services apply if the Customer has ordered the Internet Bank Access Parameters and Authorisation Tools at the Bank, or uses them.

2.2.2. The Customer agrees that the Bank is entitled to unilaterally and any time establish restrictions (access, volume of services rendered, transaction limits, etc.) for account management, conclusion and execution of Transactions via Remote Account Management Systems.

2.2.3. The Bank may terminate provision of Remote Account Management services upon at its own initiative and at any time, notifying the Customer accordingly.

2.2.4. **Connection of Remote Account Management Services**

2.2.4.1. Access Parameters and Authorisation Tools are issued to the User on the basis of the Bank's application form (Application) submitted by the Customer to the Bank; and they are activated upon a written confirmation of the receipt thereof by the User.

2.2.4.2. The User shall be provided with the Access Parameters and Authorisation Tools for the use of the Remote Account Management Services in accordance with the User's rights to manage the respective Customer's Account.

2.2.4.3. When the Customer opens new Accounts with the Bank and/or authorizes the User to manage the Account with the Bank, the User is connected to the new Account with the previously issued Access Parameters and Authorisation Tools in accordance with the User's rights to manage the respective Customer's Account.

2.2.4.4. In order to use the Remote Account Management Services, the Customer is entitled to submit to the Bank an application in the form specified by the Bank for the issue of Access Parameters and Authorisation Tools to the User, to manage various Accounts of the Customer (individual and/or legal entity). The Customer may personally submit the application as per the Bank's sample or sent it to the Bank via Remote Account Management Services.

2.2.4.5. Internet Bank is available in the following modes:

- information mode – with the User's right to view account balances/statements and other information without the right to prepare and send to the Bank Transaction Documents/Notifications;
- limited mode – with the User's right to view account balances/statements and other information and to prepare Transaction Documents/Notifications without the right to send them to the Bank,
- full mode – with the User's right to view account balances/statements and other information and the right to prepare and send to the Bank Transaction Documents/Notifications.

2.2.5. **Security and Authentication of Users**

2.2.5.1. The Bank issues Access Parameters and Authorisation Tools to the User in a sealed envelope.

2.2.5.2. Access Parameters and Authorisation Tools are confidential information that the User and the Bank undertake not to disclose and not to pass to third parties, as well as they undertake to take all required actions to prevent possible disclosure thereof to third parties.

2.2.5.3. The User undertakes to keep confidential information safe, periodically changing the Internet Bank access password.

2.2.5.4. If the Authorisation Tool was lost or stolen, codes of the Code Card, PIN code of the Digipass Device/PrivatSecure or the Access Parameters could have been disclosed to third parties, the User should promptly notify the Bank thereof verbally or in writing. Once the User's notification has been received, the Bank promptly blocks the access to respective Remote Account Management Services. The Bank notifies the User of blocking the Authorisation Tool and the reasons thereof.

2.2.5.5. If the User gives the Bank a verbal order to block the access to Remote Account Management Services, the Bank performs Authentication according to the Regulations on Providing and Receiving Information and Services via Telephone and Online Chat. The Customer should submit to the Bank a written notification regarding blocking of the respective Access Parameters/Authorisation Toolsthe verbal order.

2.2.5.6. The Bank unblocks an Authorisation Tool or replaces it with the new one, once there are no reasons for blocking thereof. According to the Customer's application submitted in the Bank's specified form, the Bank issues the Customer and activates new unique Authorisation Tools/Access Parameters in accordance with the procedure described in

these Regulations.

2.2.5.7. When the User uses Remote Account Management Services, the Bank performs the Authentication of the User by Access Parameters and Authorisation Tools.

2.2.5.8. If the Bank has reasonable concerns that the User lost control over the Access Parameters/Authorisation Tools issued by the Bank with which the User can use Remote Account Management Services, as well as upon discovery of features of signature and/or seal imprint forgery in documents confirming the receipt of the Authorisation Tools/Access Parameters, the Bank is entitled, but is not obliged to block the User's access right to the Remote Account Management Services without bearing any responsibility in this regard.

2.2.5.9. The User's access rights to Internet Bank are blocked automatically, if the Internet Bank Access Parameters are entered incorrectly 5 (five) times in a row.

2.2.5.10. The respective Authorisation tool is blocked automatically if:

- a code from the PrivatSecure c was entered or named incorrectly 3 (three) times in a row,
- a code generated by the Digipass device was entered or named incorrectly 3 (three) times in a row,
- the SMS password was entered or named incorrectly 3 (three) times in a row.

2.2.5.11. Digipass device is blocked with no recovery option if:

- the User attempted to open the Digipass device or caused mechanical damage to it,
- the PIN code was entered incorrectly 3 (three) times in a row (if using the Digipass model with the PIN code).

2.2.5.12. PrivatSecure is blocked if the PIN Code is entered incorrectly 5 (five) times in a row;

2.2.5.13. If the Customer's access to the Internet Bank and Authorisation Tools were blocked in accordance with the Regulations, the Bank can unblock them after the Bank receives from the Customer a written or verbal (via phone) application for unblocking thereof (in accordance with section 2.3. of the Regulations on Providing and Receiving Information and Services via Telephone and Online Chat).

2.2.5.14. In case of irreversible blocking of the Digipass Device for the reasons listed in Paragraph 2.2.6.11 or in case of an empty battery, the Bank replaces the Digipass Device, charging the commission fee in accordance with the Bank's Price list.

2.2.5.15. The Bank terminates a Privat24 session after 15 minutes of inactivity. Should the User repeatedly connect to Privat24, the Bank shall perform the Authentication of the User according to Paragraph 2.2.5.7 hereof.

2.2.6. **Safety Recommendations for the Use of Internet Bank**

2.2.6.1. In order to improve safety, the Customer should do the following:

2.2.6.1.1. use a personal computer, tablet, mobile phone or other safe devices (devices);

2.2.6.1.2. monitor safety updates of the operating system on the devices in use;

2.2.6.1.3. use the following software installed on the devices in use and constantly monitor the updates thereof:

- anti-virus software, firewall, and other anti-malware software;
- restrict the third parties' access to the devices without the Customer's supervision;

2.2.6.1.4. make sure the page address https://ibank.privatbank.lv and encryption certificate are authentic and valid, when using the Internet Bank (if the certificate authentication fails, the Bank should be immediately informed thereof);

2.2.6.1.5. not to save the Internet Bank password in a browser for automatic access;

2.2.6.1.6. not to keep Access Parameters in text documents that stored on devices and are freely available;

2.2.6.1.7. not to send Access Parameters to anyone be e-mail or other means of

communication;

2.2.6.1.8. not to transfer Authorisation Tools for other persons' use, including for short-term use;

2.2.6.1.9. not to keep Authorisation Tools in easily accessible places.

2.2.6.2. The Customer should bear in mind that the Bank never sends e-mails with requests to submit confidential information (Access Parameters, codes/passwords, etc.) or e-mails with software of any kind.

2.2.6.3. If the Customer suspects fraud, they should immediately inform the Bank about it.

2.2.7. **Confirmation of Transaction Documents/Notifications and Sending Thereof to the Bank**

2.2.7.1. The Customer agrees that Transaction Documents/Notifications confirmed with the User's Authorisation Tool (SMS password, code generated by the Digipass Device/PrivatSecure) in accordance with the Bank's procedure for use of Remote Account Management Services shall be deemed authentic and binding for the Customer and the Bank, and shall be deemed to be equivalent to documents executed in writing (paper form) and signed in the understanding of the Civil Law of the Republic of Latvia with full legal effect and legal consequences thereof. The Customer may not contest the Transaction Documents/Notifications sent to the Bank via Remote Account Management Service.

2.2.7.2. The Bank is entitled not execute Transaction Documents/Notifications if:

- the User violates these Regulations;
- the Transaction Document/Notification is unclear or distorted due to communication failures;
- the Bank has suspicions regarding the User's identity, and the Bank is unable to contact the User to verify their identity and content of the Transaction Document/Notification;
- the Transaction limits set by Bank have been exceeded;
- the Account does not have sufficient funds to execute the Transaction Document/Notification and to pay for the Bank's services according to the Price List.

2.2.7.3. After the receipt of the Transaction Document/Notification, the Bank is entitled, but is not obliged to contact the User and verify the authenticity of the Transaction Document/Notification.

2.2.8. **Obligations and Responsibilities of the Parties**

2.2.8.1. The Bank is obliged to:

- perform the Authentication of the User in accordance with provisions of these Regulations;
- ensure provision of Remote Account Management Services in accordance with provisions of these Regulations, the Bank's Price List, and Payment Execution Regulations.

2.2.8.2. The Customer is obliged to:

- familiarise the User with provisions of the Regulations;
- at least once a month, verify the compliance of executed Transactions in the Account statement and review the Bank's notifications addressed to the Customer in the Internet Bank.

  If the Customer orders the Bank to send the Access Parameters / Authorisation Tools to the User by post and/or hand them over via third persons, the Customer shall be aware of and undertake all risks related to sending the Access Parameters / Authorisation Tools, including those concerning safety and delivery

time of postal items. The Bank is entitled to use services of third persons to execute the Customer's order to deliver the Access Parameters / Authorisation Tools. The Bank is not liable for losses or other expenses of the Customer or third persons, which may occur in case of late delivery, loss, misuse, lack or damage of the Access Parameters / Authorisation Tools, disclosure of confidential information, or in the result of any other circumstances beyond the Bank's control.

2.2.8.3. The Bank shall not be financially liable:

- in case the User does not comply with the Regulations;
- for losses that the Customer incurs/may incur due to damages or failures of communication channels or in cases when Remote Account Management Services or individual functions thereof are for technical reasons unavailable to the User for execution of Transactions, and/or in case a Transaction Document/Notification has not been received by the Bank;
- for losses the Customer may incur due to changes to User rights, if the Bank acts in accordance with the User's Notifications, including in case the Bank establishes that the User has violated the provisions of decision-making process;
- for any losses that the Customer incurred or may incur when submitting the Transaction Document/Notification to the Bank via the Remote Account Management Services;
- for the Customer's losses in case unauthorised (third) parties use the Access Parameters/Authorisation Tools issued to the User and the User has failed to promptly notify the Bank thereof;
- for execution of Transactions, including debiting of funds from the Customer's accounts in accordance with forged or otherwise illegally executed Transaction Documents/Notifications if such documents were confirmed with the Authorisation Tools/Access Parameters issued to the User.

2.2.8.4. The Bank is responsible for execution of unauthorised Transaction Documents/Notifications, unexecuted or erroneously executed Transaction Documents/Notifications in the amount specified in the particular section of the Regulations. The procedure for the submission and consideration of the Customer's claims and complaints with regard to execution of a non-authorised Transaction document/Notification is specified in Section 1.1 – 'Terms, Definitions and Principal Conditions of General Regulations for Transactions'.

2.2.8.5. The Customer is responsible for:

- authenticity, precision, and completeness of the information specified by the Customer in the Application using Remote Account Management Services;
- precision and completeness of the User's orders, as well as for the User's actions, and undertakes to cover all losses of the Bank resulting from the User's actions;
- compliance with the Regulations.

2.2.8.6. The Customer undertakes all risks and responsibility for losses resulting from:

- incorrect or distorted transfer of Transaction Documents/Notifications, including misunderstandings, errors, or distortions caused by lack or failures of the communication infrastructure, except where the losses incur due to the Bank's serious negligence;
- illegal actions of third parties until Remote Account Management Services were blocked in accordance with the procedures described in Paragraphs 2.2.5.4–2.2.5.6;
- duplication of a Transaction Document/Notification;
- non-compliance with these Regulations.

2.2.9. **Copyright, Alterations**

2.2.9.1. All personal rights and copyright to Internet Bank and materials related thereto belong to the Bank. The User may use the Internet Bank only within the framework specified in these Regulations and in accordance with provisions determined by the Bank.

2.2.9.2. Any alterations of the Internet Bank, any reproduction, publishing, transfer to third parties, and use of the Internet Bank technologies not specified in these Regulations for the purposes of creation of other software with functions of the Internet Bank without the Bank's consent are prohibited.

2.2.10. **Commission Fees**

2.2.10.1. The Customer shall pay the Bank Fees for the use of the Remote Account Management Services, issue and replacement of Access Parameters/Authorisation Tools in accordance with the Price List, as well as in other cases determined in the Price List.

2.2.10.2. The Bank shall deduct respective Commission Fees in accordance with the Price List from the Customer's Accounts with the Bank on an uncontested basis and without receiving the Customer's consent for such action, or the Customer shall pay them in cash at the Bank.