

Recommendations for the safe use of Paysera system

General provisions

1. The present Recommendations for the safe use of Paysera system (hereinafter referred to as Recommendations) is a supplement to the General payment service agreement which enters into force together with the General payment service agreement.
2. When visiting the present website and/or using services the Client acknowledges and confirms that s/he has read and understood the present Recommendations.

Using the System

3. To log in to the Paysera account in the System the Client uses their email address or phone number and a password of at least 8 symbols. After logging in to their Paysera account with the aim to use Paysera services the Client shall additionally confirm their login.
4. Additional login confirmation is performed as follows (the methods are listed from the least to the most safe):
 - 4.1. by receiving a single use code to the email address confirmed in the System and entering it to a special field in the Account;
 - 4.2. by receiving a single use code to the phone number confirmed in the System and entering it to a special field in the Account;
 - 4.3. via multilevel login systems of third parties (e.g. online banking);
 - 4.4. with the help of a qualified electronic or mobile signature.
5. The method of additional login confirmation is chosen by the Client. Upon reaching a turnover of 50 EUR or more on the account, the Client is recommended not to use email address for additional login confirmation.

Safety recommendations

Password

6. Login password to the Account in the System shall be unique and consist of at least 8 symbols, including capital and small letters, numbers and special symbols.
7. The password shall not include information about the Client or his/her family members which can be known or easily accessed by third persons, such as: birth dates, names, surnames or pet names of family members or friends or their fragments. Also, it shall not consist of easily memorable and/or guessable combinations of numbers and letters.
8. The password shall not be used for logins to other systems, accounts, etc., i.e. it shall be unique and not used anywhere else.
9. The Client shall remember the password and shall not write it down in his/her notebook, sticky note or anywhere else, shall not enter it in his/her mobile phone, email or other electronic means of communication, and shall not reveal or otherwise transfer it to third persons. The password may not be remembered if the Client uses special and appropriately secured programs for password storage or generation or administration. The Client shall him/herself enter and choose appropriate password storage methods and instruments. The Client him/herself is responsible for password safety.
10. The password used to log in to the Account shall be changed at least once in 3-6 months (the System, in dependence on the difficulty of the password and usage statistics, requests to change the password when the terms comes to an end).
11. Paysera does not initiate notifications (via SMS messages, emails, calls, etc.) with the offer or request to change the password or links to the password reset page. If the Client receives such notification, s/he shall immediately inform Paysera thereof. The password can be changed by logging in to the Account in the System or directly on Paysera website under relevant procedures. If the Client receives such notification, s/he can be sure that it is not fraud only if the Client has used password reminder in the System.
12. If any suspicions arise that the password may be known to third persons, the Client shall immediately change it and then check for illegal logins to the Account and performed or initiated illegal payment operations.

Additional login confirmation

13. Email used for additional login confirmation shall be secured with a unique password of at least 8 symbols, including capital and small letters, numbers and special symbols. Also:
 - 13.1. The password shall not be used for logins to other systems, accounts, etc.;
 - 13.2. The Client shall remember the password and shall not write it down in their notebook, sticky note or anywhere else, shall not enter it in their mobile phone, email or other electronic means of communication, and shall not reveal or otherwise transfer it to third persons;
 - 13.3. If any suspicions arise that the password may be known to third persons, the Client shall immediately change it.
14. Email used for additional login confirmation shall be used only by the Client.
15. If the Client notices any suspicious activity on their email account used for additional login confirmation (logins are performed from unknown IP addresses, emails are not received, etc.), s/he shall immediately check for illegal logins to the Account. If the Client notices illegal logins to the Account, s/he shall immediately inform Paysera thereof and change email and Account passwords. The Client is also recommended to change the additional login confirmation method to a more safe one.
16. The Client shall have a continuously updated anti-virus program installed on their device.
17. Mobile phone used for login confirmation shall be secured with a lock (PIN code, password, lock pattern, etc.).
18. If the Client losses the mobile phone used for login confirmation, s/he shall immediately block their SIM card.
19. The Client who uses online banking or qualified electronic signature for login confirmation shall undertake all measures to prevent these instruments from being accessed by third persons and/or used for login confirmation by third persons.

Account

20. The Client shall log in to the account safely: in order to log in to the Account, the Client shall open a new browser window and enter the address https://www.paysera.* (the list of valid domains can be found here). The Client shall always make sure that the internet address is www.paysera.* and the certificate used on the page is issued by Paysera. If any other domain is used or the HTTPS protocol is not used, it is highly probable that the website is not real and logins to such website are forbidden.

21. After completing their actions on the Account, the Client shall log out from the System and shall not leave the Account accessible to third persons.

22. It is not recommended to log in to the Account via public computers or devices of other persons.

23. The Client is recommended to at least once a month check the IP addresses used to log in to the Account.

24. If the Client usually logs into the Account only from home and/or work and there is no need to log in from other places, it is recommended to restrict logins to the Account to specific IP addresses. It is recommended to set at least 2 such IP addresses.

25. The Client shall update his/her contact information on the Account in time (including but not limited to phone number and email address), so that Paysera could contact the Client and/or identify him/her.

26. The Client shall execute all reasonable instructions provided in the System, related to safety of payment instruments.

27. If the Client notices any suspicious activity on their Account and thinks that third persons may have logged in to the Account, the Client shall:

27.1. immediately inform Paysera thereof and request to block the Account;

27.2 in order to continue to use the Account, the Client shall change the Account password, use other additional Account confirmation instruments or use safer instruments and delete unsafe additional login confirmation instruments from their Account.

Used devices / software

28. The Client is responsible for safety of devices used to log in to the Account, shall not leave them unattended, in public places or otherwise easily accessible to third persons.

29. It is recommended to update software, applications, anti-virus programs, browsers and other programs in time.

30. It is recommended to protect devices with passwords, PIN codes or other safety instruments.

31. The Client shall use only original software and its standard instruments provided with the device and shall not perform any amendments to the system files. If any other software is installed on the device or its standard integrated rights and protection features or system files are amended, the risk to the security of data stored by separate installed applications increases.

32. The Client is forbidden to use features which allow to save login data on the device or browser.

Other advices

33. The Client can manage their Paysera account also via Paysera application. To log in to the application the Client will have to enter their Account password; thus, the Client has to make sure that Paysera application has been downloaded from official websites (Apple Store, Google Play, Windows Phone Store). It shall be noted that Paysera application is one of the payment instruments, which means that the Client, when using the application, shall observe relevant safety requirements, just like s/he does when using their Account.

34. It is recommended to be careful when submitting the following personal data online: name, surname, legal person name, identification codes, email address, phone number, passwords, financial information (payment cards, account numbers, PIN codes, etc.), personal document number, etc. The Client is strictly forbidden to enter data of his/her Paysera payment instruments to systems of third persons with the aim to enable the third person to perform a payment on behalf of the Client from the Account of the Client (i.e. use Paysera system emulators). If such activity of third persons is established, the payment operation may be suspended, the access of the Client to the Account may be restricted and/or provision of services may be suspended.

35. The Client shall undertake necessary safety measures in order to prevent third persons from seeing passwords, PIN codes, login codes and other personalized safety attributes entered by the Client.

36. It is recommended to evaluate received emails with cautiousness, even if Paysera or Paysera is indicated as the sender. Paysera will never request the Client to download attachments or install software. Attachments to fraud emails may contain viruses which can harm devices or pose a risk to the safety of the Account.

37. It is recommended not to click on unknown links, open unknown documents, install software or application from unknown, unreliable sources or visit unsafe websites.