PPF BANKA A.S. – SECURITY PRINCIPLES FOR ELECTRONIC BANKING

The Bank shall not be held liable for any data loss, Personal Data leakage, or any other facts caused by failure to respect the recommendations set out in this document.

User support for Electronic banking ("ELB") is provided by Customer Service. The contact details of the Customer Service and its Business hours are available on the bank's website.

1. Visit only known websites. Use only secure passwords and protect them thoroughly.

Whenever you visit a website, check whether the domain corresponds to the content of the website.

Use only trustworthy services and always make sure that you really are communicating with the correct server.

Use strong passwords – at least 8 characters, and a combination of lower case and upper case letters, numerals and special characters when accessing your e-mail accounts, social network accounts etc.

Do not use the same passwords for several services. Use a password manager.

Use multi-factor authentication on all services and apps where possible. Multi-factor authentication significantly increases the security of your personal and financial data.

2. Do not open e-mail messages from unknown senders or with a suspect name. Download and open only the files that you expect and that arrive from known senders.

Do not open attached files and do not click on links in unknown e-mail messages and **never disclose sensitive data in response to an e-mail message received**. Do not download and open files with unknown content.

The Bank never sends unsolicited messages containing links to its website and it never uses such messages for requesting the submission or disclosure of ELB login data.

Check any unusual e-mails from your business partners over the telephone, in particular if they are related to a payment account change. Also check such changes even if they come from a familiar e-mail address.

There has recently been a surge in attempts to fraudulently obtain login data through fake websites (phishing), text messages (smishing), and telephone calls (vishing).

The Bank never requires you to disclose your login credentials or verification codes, or to install any software via phone, e-mail, or SMS.

If you do receive such a request, immediately terminate the communication and contact the Bank's Customer Service.

3. Use multi-factor authentication on all services and apps where possible. Multi-factor authentication significantly increases the security of your personal and financial data.

- Android 14 or higher
- Apple iOS 18 or higher
- Windows 11 or higher
- MacOS 18 or higher

These versions of the systems provide the latest security updates and protection against cyber threats, ensuring a more secure login to Internet Banking (hereinafter referred to as "IB"), Mobile Banking (hereinafter referred to as "MB"), e-Token and Client API (hereinafter referred to as "API"). Older versions of these systems no longer receive regular security updates from their manufacturers, making them more susceptible to abuse.

4. **Before installing or updating your Mobile Banking or e-Token, always verify that the application is officially provided by "PPF banka a.s." in Google Play or the App Store.**

   Never install applications from unknown sources that purport to be PPF banka apps.

5. **Install anti-virus software and anti-spyware and activate the regular updates of this. Install important updates of applications, in particular those of the operating system.**

   Install available updates of the operating system, browsers, and all the programs and applications that you have installed, on all the devices that you use.

   Use only legal versions of software; illegal versions may contain viruses, Trojan Horses and other malware. Such programs can, for example, send your passwords to their authors. Download programs to your computer from the manufacturer's website. Only install applications from official sources (Google Play, Apple Store, and Windows Phone Store) to your mobile phone.

   Restrict other people's access to your computer. Never use a publicly accessible computer to access tablet or mobile phone to access the API, IB or MB.

   Never connect media (USBs, flashdisks, memory cards, CDs, DVDs, etc.) that are unknown or that you have found to your computer or mobile telephone.

   If you store documents containing financial or personal data (such as statements or payment confirmations), we recommend protecting them with a password or encrypted storage.

   Do not send confidential information by e-mail without encryption or another form of protection.

6. **For everyday work, in particular for working with the internet, do not use a user profile with administrator rights. Do not make it possible for other people to connect to the network via your own user profile.**

   Log into your computer as a normal user and log in using administrator rights only when absolutely necessary. **Before leaving your computer, always lock the screen or terminate all connections with API and log out of IB application.**

7. **Only launch IB on a known computer and from the link on the Bank's homepage. When accessing IB, check whether the connection is properly secured and communicate with the Bank.**

   When you have to use an unknown computer close all browser windows, then open a single new window in the browser before logging into IB. Erase the history of your viewing and close the window in the browser after logging out of IB.

   Do not connect to the Internet via public wi-fi networks, use your operator's mobile data or trusted Wi-Fi networks.

8. **Use biometrics to access MB.**

9. **To store a Signature Certificate to the API, use a secure storage that requires a password or PIN to access this certificate.**

10. **Check movements in your accounts and payments by your Debit card on a regular basis; in IB, set up the sending of SMS or e-mail notifications of selected events, enable push notifications in MB and on your phone.**

    In IB, you can set up the sending of notifications of the User's logins into IB, of the transactions made in Accounts and with Debit cards, etc. **It is also possible to set up the sending of notifications to persons other than IB Users,** for example, to accountants or Debit card Holders.

    In MB you can enable push notifications for the same events as in IB.

11. **Set up Limits for Payment Orders for the Users. In IB, allow at least one User to authorise requests for the Client.**

    You can set up Time-based Limits and Transaction Limits, and combinations of these.

    In IB, a User holding the right to authorise requests for the Client can also request the blocking of other Users in the case of any suspicion of IB abuse; such blocking will be carried out in a matter of minutes. We therefore recommend to also assign that authorisation to at least one IB User.

12. **Pay attention to whether you are really authorising the Payment Order or the request to the Bank that you have submitted.**

    Before confirming them, always first check the data for accuracy (for example, by comparing the data against the invoice, postal money order etc.), in particular payment details stated in the authorisation SMS.

13. **Protect the Security Elements. Do not disclose your login data to anyone and prevent the theft of this data when you are entering it. Change your Login Passwords for ELB on a regular basis.**

    Treat all documents from the Bank (such as contract documents, envelopes with login names and passwords for ELB etc.) as confidential and keep them in a secure place. **If you allow anyone to have access to your personal data or Security Elements, you give this person an opportunity to abuse such data or disclose such data to another person**.

    When creating your login password for ELB do not use easily intelligible information such as names, dates of birth, telephone numbers etc.

14. **Have the mobile phone intended for sending SMS codes for IB or with the e-Token and/or MB installed on with you at all times. Store the e-Token, in a safe place when you are not currently using it.**

    Protect the data in your mobile phone memory by a PIN code or other protective features available in the particular handset. Secure access to MB with a PIN or biometrics. For the highest security, store the Token in a lockable cabinet.

    Do not interfere unlawfully with the operating systems of mobile telephones (so-called Jailbreak or root) and do not acquire any such mobile phones.

15. **Pay due attention to the messages on your computer and on the Bank's website, and follow them.**

16. **Do not hesitate to contact the Bank in the case of any doubt or strange behaviour of the computer when you are logging into ELB or accessing other services, in particular:**

    - when you receive an e-mail message containing a link to the Bank's website;
    - in the case of suspicion of the disclosure of login data;
    - if your computer is infected or a ransomware is detected on your computer;
    - in the case of suspect behaviour of ELB, for example, SMS codes not arriving, the SMS code contains different data about the payment, an unusual name of the server, a different visual impression, new steps during login, etc.;
    - when you lose the Token or the mobile phone for receiving SMS codes or in which the e-Token is installed;
    - when you find discrepancies in the executed Payment transactions.

17. **How to protect yourself:**

    - Do not share sensitive data unless you are certain who you are communicating with.
    - Do not send payments to an account whose true owner you do not know.
    - If you have any doubts or suspicions, verify that the person contacting you really is who they claim to be by checking their telephone number or email address.

18. **Final provisions**

    These Security Principles come into force and effect on 11 November 2025 and supersede the existing Security "Principles for the Electronic Banking of PPF banka a.s." in force since 2 March 2025.

PPF banka a.s. | Evropská 2690/17 | P.O. Box 177 | 160 41 Praha 6
T +420 224 175 888 | F +420 224 175 980 | info@ppfbanka.cz | www.ppfbanka.cz

Registrováno Městským soudem v Praze, oddíl B, vložka 1834 | IČ 47116129 | DIČ CZ47116129