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 who can be contacted on Business Days between 8 a.m. and 6 p.m. on telephone number +420 224 175 901 for Internet banking ("IB") and API, or +420 224 175 995 for Homebanking ("HB"), or via e-mail at customer.service@ppfbanka.cz

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 provider.

   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.

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.

3. **Install anti-virus software and anti-spyware and activate the regular updates of this. Install important updates, 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.

   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. Download applications from official sources (Google Play, Apple Store, and Windows Phone Store) to your smart phone.

   Restrict other people's access to your computer. Never use a publicly accessible computer to access API, IB or HB.

4. **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 IB, or terminate your work in HB and close down the whole application.**

5. **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 erase the history of your viewing after logging out of IB.

6. **Do not store the HB Signing Certificate in your computer but on a USB disk, which you disconnect from the computer upon terminating your work with HB.**

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

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, E: info@ppfbanka.cz
www.ppfbanka.cz

PPF Banka

8. **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.**

   In IB, you can set up the sending of notifications of the User's logins into IB, of the transactions made in Accounts and on payment cards, etc. **It is also possible to set up the sending of notifications to persons other than IB Users,** for example, to Debit card holders. For details please see Part III of the User Guide for IB.

9. **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. You can find details about the requests in the Business Conditions of PPF banka a.s. for the Internet banking and in Part III of the User Guide for IB.

10. **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.).

11. **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.

12. **Have the mobile phone intended for sending SMS codes for API or IB on you at all times. Store the OTP Token, or the USB disk with the Signature Certificate for HB, 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. For the highest security, store the OTP Token or USB disk in a lockable cabinet.

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

14. **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 OTP Token or the mobile phone for receiving SMS codes;
    - when you lose the USB disk on which the Signature Certificate is stored;
    - when you find discrepancies in the executed transactions.

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, E: info@ppfbanka.cz
www.ppfbanka.cz