# Rules of Using FortiPay

**Rules of Safe Behaviour on the Internet and Using FortiPay**, a Web Means of Payment.

**Recommendation for Clients.**

1. **Only you know your security data and nobody else**

Do not disclose your security data to the web means of payment (hereinafter referred to as "*Internet Banking*") to any person, particularly your user´s number, login data, password, access code, and do not send them by e-mail or by means of social networks. Particularly, mind your privacy when logging in and make sure that any other people cannot see your login data. Also do not leave your computer or mobile phone unattended, use keyboard locks and access codes to the devices. Avoid using the products of internet banking in the public (e.g. in public transport) or in any monitored rooms (e.g. within the reach of security cameras).

2. **Mind where you access your internet banking from**

Do not use internet banking on computers of which you cannot be sure whether they are free of malicious programmes. Certainly avoid using any public computers in internet cafés or at airports and in information centres. If possible, use only your computer or mobile phone to access your Internet Banking. Always check in the browser header whether you use the secured link to access your Internet Banking. It is simple, the site always starts with https:// (the "s" at the end is important), or the browser itself may notify you of it by green colour or the symbol of the locked lock before the name of the website.

3. **Beware of unknown links and websites**

Visit only known and trusted Internet websites. Today´s attackers are ingenious and are able to reproduce very accurately, for instance, a login site to Internet Banking, and smartly lead you to it. Therefore, beware of any unknown links on the Internet and in e-mail which could lead you to sites resembling a login form to Internet Banking, e-mail or social networks, for instance. If you consider the login site to Internet Banking products suspicious in any way, do not log in. Make sure and check in the browser header whether you actually are on the particular website and not a false one.

The sites with erotic contents or for software, video and music download can be especially dangerous, often containing a lot of malicious software and viruses.

4. **Suspicious e-mail? Do not open it, rather delete it.**

The Company never sends e-mails requesting identification data, user´s number, login, passwords, PINs, authorization codes, data to a payment card, etc.. Never respond to such requests. In your e-mail box open only trustworthy e-mails from known and expected senders. If an e-mail seems suspicious in any way, rather delete it immediately. If you have already opened it, certainly do not open attachments and links it contains. And if you click on such a link or open an attachment accidentally, immediately close it and do not allow the programme or browser to install anything. ,Subsequently, we recommend that you check your computer or mobile phone by anti-virus software.

5. **Protect yourself against spams**

The best tool to eliminate majority of unsolicited and dangerous mail is to set up and actively use e-mail spam protection. Most public services as well as many e-mail clients as Outlook and others offer such protection. Its setting-up is often intuitive and simple. Also consider using further security programmes such as antispyware and antiadware which protect you from unsolicited advertisements and dangerous programmes.

6. **Use and update your antivirus programmes and firewall both in your computer a on your mobile phone**

Check your device regularly by means of an antivirus programme. Never turn off your antivirus programme; do not forget to update it regularly (it is possible to set up automatic updating via the Internet) and use its latest version with implemented protection and detection of malicious software. Criminals never sleep; the older your antivirus programme is, the less effective it is against new threats. We also recommend that you should use firewall on your computer. Get antivirus also for your mobile phone. It is very dangerous to think that phones cannot be attacked by viruses; you might pay dearly for that assumption. If you have any suspicion that your computer or mobile phone has been attacked by a virus, do not use it to access your Internet Banking or other services containing your personal data (e-mail, social networks, Internet shops, etc.) and contact an IT specialist.

7. **Update your devices, your computer and mobile phone**

Update your programmes and operation systems regularly, too. It is particularly important to update the Internet browser in your computer and mobile phone and all its so-called plug-in modules (e.g. Flash player). Also update all your security programmes. Check for released operation system patches and do not delay their installation. As to smartphones or tablets we recommend that you should use the latest version of the operation system (the so-called firmware) officially offered by the device manufacturer. All old versions of your programmes pose potential threat to safe browsing and thus to your finance. Never install any programme, the origin of which is not known to you, into your computer or mobile phone. Install on your mobile phone only applications from official application stores - Google Play (Android), App Store (iOS), Windows Marketplace (Windows Phone).

8. **Know your balance and transactions, notify the Company of any discrepancy**

The best early warning tool to find out that anything is out of the ordinary is to know the balance of your account and the transactions you have made. If you notice any transaction you have not made, or you are doubtful about correctness of the balance of your account, immediately contact the Company line at +420 558 335 000 and e-mail devizy@devizy.cz. Do not postpone such reporting, please! Only fast reply might prevent you from other loss and find fast solution.

9. **Regularly check for news about the Internet security**

The more information you have, the safer you can behave on the Internet. Regularly check for latest news in the sphere of the Internet security and follow all the recommended rules.