**Rules for safe use of the Internetbanking CYRRUS FX payment instrument Recommendations for clients.**

1. **You and you alone know your security data.**

Never share your security data for the online payment instrument (hereinafter referred to as “Internet banking”) with anyone else, meaning in particular user number, login, password, PIN and authorisation code, and never send them by e-mail or via social networks. Pay attention to your privacy, especially when logging in, and make sure that other persons are unable to see your login data. In the same way, do not leave your computer or mobile telephone unattended, use keyboard locks and access codes to devices. Avoid using Internet banking services in public (for example, on means of public transport) or in monitored areas (for example, in view of security cameras).

1. **Watch where you access Internet banking.**

Do not use Internet banking on computers in which harmful programs might be installed. Absolutely avoid any public computers in Internet cafes or at airports and in information centres. If possible, only use your own PC or telephone to log into Internet banking. Always check in the header of the browser whether you are accessing Internet banking via a secure connection. This is easy to check: the page begins https:// (the “s” at the end is important); otherwise the browser itself will notify you of this (in green or with the symbol of a locked padlock in front of the name of the website).

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

Only visit known and trustworthy pages on the Internet. Today’s attackers are inventive and are able to very faithfully reproduce a login page for Internet banking and direct you there. For this reason beware of any unknown links on the Internet and in an e-mail that might take you to pages that look like the login form to Internet banking, an e-mail or, for example, social networks. If the login screen for Internet banking products seems suspicious to you in any way, do not log in. To be on the safe side, always check in the browser header whether you are actually at the right website and not a fake one (Cyrrus FX Internet banking has its site at https://ib.cyrrus-fx.cz/login/).

Sites containing sexual content or sites at which you can download software, videos and music can be particularly dangerous and often contain a lot of dangerous software and viruses.

1. **Suspicious e-mail? Do not open and delete.**

The company will never send you e-mails asking you to share identification details, user number, login, password, PIN, authorisation code, payment card details, etc. Never respond to such requests. Open only trustworthy e-mails from known and expected senders in your inbox. If an e-mail seems suspicious in any way, it is best to delete it. If you have already opened it, certainly do not open the attachments and links which it contains. And if you accidentally click on a link or open an attachment, quickly close it and do not allow the program or the browser to install anything. We suggest you then check the computer or mobile device with antivirus software.

1. **Protect yourself against spam.**

The best way of eliminating most unsolicited and dangerous mail is to set and actively use anti-spam e-mail protection. Most public services offer this, as do many e-mail clients, such as Outlook and others. Set-up is often intuitive and simple. Consider using other security programs, such as anti-spyware and anti-adware, to protect you from unwanted advertisements and dangerous programs.

1. **Use and update the antivirus program and firewall on your computer and telephone.**

Regularly check your devices using an antivirus program. Never switch off your antivirus program, do not forget to regularly update it (automatic updates can be set up over the internet) and use the latest version with implemented protection and harmful software detectors. Fraudsters never sleep, meaning the older the antivirus program, the less effective it is against new threats. We also recommend that you use a firewall on your computer. Install an antivirus program in your mobile telephone as well. It is a dangerous myth that viruses do not attack telephones and one that you might regret believing. If you suspect that your computer or mobile telephone has been attacked by a virus, do not use it to access Internet banking or for other services involving your personal data (e-mail, social networks, e-shops, etc.) and contact an IT specialist.

1. **Update your devices, computer and mobile telephone.**

Regularly update your programs and operating systems as well. It is particularly important that you update the web browser on your computer and telephone and all plug-in modules (for example, Flash Player). Update all your security programs as well. Keep an eye on operating system fixes and install them right away, not “later”. We recommend using the latest versions of the operating system for smartphones and tablets which the manufacturer officially offers for the device (“firmware”). All old versions of your programs pose a potential threat to secure surfing and to your money. Never install programs whose origins you do not know on your computer or telephone. Only install applications on mobile telephones from official app stores, for example Google Play (Android), App Store (iOS) and Windows Marketplace (Windows Phone).

1. **Keep an eye on your balance and on transactions and report discrepancies to the company.**

Know how much money remains in your account and which other transactions you have carried out - it is the best way of finding out that something is not right on time. If you find any operation that you have not carried out or if you have doubts as to the correctness of the balance in your account, immediately contact the company by telephone at +420 221 592 388 or by e-mail at FXinfo@cyrrus.cz. Please do not delay reporting this to us! Only a fast response can prevent any further losses or can enable us to find a fast solution.

1. **Regularly keep an eye on Internet security news.**

The more information you have, the safer you will be on the Internet. You should therefore regularly check the latest news on Internet security and stick to all the recommended rules.