SECURITY INSTRUCTIONS FOR USING ONLINE BANKING

1. Principles of safe behaviour on the Internet and in Internet Banking (hereinafter referred to as "IB")

- ✓ Make sure you are on the official website of the company.
- ✓ We are only able to ensure your security on our official site by encrypting your communications.
- ✓ Please only log in to online banking via the official website.
- ✓ For more information, please visit https://www.paymont.eu/

1.1 Passwords - basic security instructions

- ✓ Do not write down your password, do not disclose it to others and change it regularly.
- ✓ A secure password should not contain a commonly used word, name, your personal data, etc. Choose a combination of alphanumeric characters to create a secure password.
- ✓ Do not disclose your online banking password to anyone over the phone or by email.

1.2 Internet banking - basic security instructions

- ✓ Please log in to Online Banking only via the official website https://ib.paymont.eu.

BEZPEČNOSTNÍ POKYNY PRO UŽÍVÁNÍ INTERNETOVÉHO BANKOVNICTVÍ

1. Zásady bezpečného chování na internetu a v internetovém bankovnictví (dále jen „IB“)

- ✓ Ujistěte se, že se nacházíte na oficiálních stránkách společnosti.
- ✓ Vaši bezpečnost jsme schopni zajistit pouze na našich oficiálních stránkách, a to díky šifrované komunikaci.
- ✓ Do internetového bankovnictví se přihlašujte pouze přes oficiální webové stránky.
- ✓ Další informace najdete na stránce https://www.paymont.eu/

1.1 Hesla – základní bezpečnostní pokyny

- ✓ Heslo si nikam nezaznamenávejte, neprozrazujte ho dalším osobám a pravidelně jej měňte.
- ✓ Bezpečné heslo by nemělo obsahovat běžně používané slovo, jméno, vaše osobní údaje apod. Pro vytvoření bezpečného hesla zvolte kombinaci alfanumerických znaků.
- ✓ Přístupové heslo do internetového bankovnictví nesdělujte nikomu po telefonu, ani nezasílejte e-mailem.

1.2 Internetové bankovnictví – základní bezpečnostní pokyny

- ✓ Do internetového bankovnictví se přihlašujte pouze přes oficiální webové stránky https://ib.paymont.eu.

- ✓ Please follow the security instructions regarding your access data or your passwords.
- ✓ Do not lend your mobile phone to anyone and do not leave it unattended.

1.3 General information, e-mail communication

- ✓ PAYMONT? NEVER requires a password for Internet Banking.
- ✓ PAYMONT does NOT send password change information by email, nor does it EVER requires any other authentication via e-mail.
- ✓ PAYMONT uses the email address support@paymont.eu to communicate with you.
- ✓ PAYMONT NEVER sends links to the online banking login pages.
- ✓ PAYMONT NEVER requires the client to send or confirm their identification, disclose of a password or PIN for a credit card.

1.4 Mobile phones

- ✓ PAYMONT NEVER sends any security or other certificates to a client's mobile phone that you would have to install.
- ✓ PAYMONT NEVER asks for certificates or security applications to be installed on mobile phones.

- ✓ Dodržujte bezpečnostní zásady týkající se Vašich přístupových údajů nebo hesel.
- ✓ Nikomu Nepůjčujte svůj mobilní telefon a nenechávejte ho bez dozoru.

1.3 Všeobecné informace, e-mailová komunikace

- ✓ Společnost PAYMONT? po Vás NIKDY nevyžaduje heslo do internetového bankovnictví.
- ✓ Společnost PAYMONT NEZASÍLÁ údaje o změně hesla e-mailem, ani NIKDY nepožaduje jiné ověření prostřednictvím e-mailu.
- ✓ Pro korespondenci s Vámi využívá společnost PAYMONT adresu support@paymont.eu.
- ✓ Společnost PAYMONT NIKDY nezasílá odkazy na stránky sloužící k přihlášení do internetového bankovnictví.
- ✓ Společnost PAYMONT NIKDY nevyžaduje zaslání nebo potvrzování identifikace klienta, sdělení hesla nebo PIN kódu k platební kartě.

1.4 Mobilní telefony

- ✓ Společnost PAYMONT NIKDY nezasílá na mobilní telefon klienta žádné bezpečnostní ani jiné certifikáty, které byste museli instalovat.
- ✓ Společnost PAYMONT NIKDY nežádá o instalaci certifikátů nebo bezpečnostních aplikací v mobilních telefonech.

2. Basic information about the security of your computer

- ✓ Make sure your internet browser is up-to-date.
- ✓ Use anti-malware programs, i.e. anti-virus software, etc.
- ✓ Update your operating system regularly.
- ✓ Do not download suspicious programs, illegal copies (warez) or applications enabling illegal use of programs (cracks).
- ✓ Protect your computer from unauthorized interference by unauthorized persons.
- ✓ The use of file sharing programs (P2P, torrents) is a security risk and should be associated with increased vigilance.
- ✓ If possible, use a strong password or other standard method such as fingerprint or hardware keys to log in to your computer.

2.1 Mozilla Firefox internet browser

If you use Mozilla Firefox for your work, here is one of its secure settings:

- ✓ Click on the menu button ☰ and select *Settings*.
- ✓ Go to the Privacy and Security section.
- ✓ From the drop-down menu next to the text *Browsing history*, choose to Use custom setting for history
- ✓ Uncheck the *Remember search and form history option.*
- ✓ Close the page. Any changes you have made will be saved automatically.

Turn off the password management feature:

By default, Firefox offers to remember usernames and passwords. How to change this setting:

2. Základní informace k bezpečnosti vašeho počítače

- ✓ Provádějte pravidelné aktualizace Vašeho internetového prohlížeče.
- ✓ Používejte programy proti malwaru, tj. antivirový software apod.Provádějte pravidelné aktualizace Vašeho operačního systému.
- ✓ Nestahujte podezřelé programy, nelegální kopie (warez) či aplikace umožňující nelegální využívání programů (cracky).
- ✓ Chraňte svůj počítač před neoprávněnými zásahy cizích osob.
- ✓ Používání programů ke sdílení souborů (P2P, torrenty) je bezpečnostním rizikem a mělo by být spojeno se zvýšenou ostražitostí.
- ✓ Pro přihlášení k Vašemu počítači používejte pokud možno silné heslo, nebo jinou standardní metodu jako je otisk prstu nebo hardwarové klíče pro přihlášení.

2.1 Internetový prohlížeč Mozilla Firefox

Pokud pro svou práci používáte prohlížeč Mozilla Firefox, zde uvádíme jednu z možností jeho bezpečného nastavení:

- ✓ Klikněte na tlačítko nabídky ☰ a zvolte Nastavení.
- ✓ Přejděte do sekce Soukromí a zabezpečení.
- ✓ Z rozbalovací nabídky u textu *Historii prohlížení* zvolte ukládat podle vlastního nastavení.
- ✓ Zrušte zaškrtnutí volby *Pamatovat si historii hledání a formulářů.*
- ✓ Zavřete stránku. Všechny provedené změny budou automaticky uloženy.

Vypnutí funkce správy hesel:

1. Click the menu button and select *Settings*.
2. Go to the *Privacy & Security* section and find the *Login and Passwords* section.
3. If you want Firefox to stop saving usernames and passwords on all sites, uncheck the *Ask to save logins and passwords for websites.*

For information on updating (usually automatically) and the latest browser versions, please visit https://www.mozilla.org or http://www.mozilla.cz.

Ve výchozím nastavení Firefox nabízí zapamatování uživatelských jmen a hesel. Jak toto nastavení změnit:

1. Klikněte na tlačítko nabídky ☰ a zvolte *Nastavení.*
2. Přejděte do sekce *Soukromí a zabezpečení* a najděte část *Přihlašovací údaje.*
3. Chcete-li, aby si Firefox přestal ukládat uživatelská jména a hesla na všech webech, zrušte zaškrtnutí volby ***Ptát se na ukládání přihlašovacích údajů.***

   Informace o aktualizaci (většinou probíhá automaticky) a nejnovějších verzích prohlížeče se dozvíte na stránkách https://www.mozilla.org nebo http://www.mozilla.cz.

2.2 The Windows operating system in general

Users of the MS Windows operating system are advised to follow the Windows Security warnings and information, or visit https://www.microsoft.com/en-gb/security or https://www.microsoft.com/cs-cz/security and follow the recommendations published there.

2.2 Operační systém Windows obecně

Uživatelům operačního systému MS Windows doporučujeme sledovat varování a informace aplikace *Zabezpečení Windows*, případně navštívit webové stránky https://www.microsoft.com/en-gb/security nebo https://www.microsoft.com/cs-cz/security a řídit se zde publikovanými doporučeními.

3. User Support

In case of any questions from clients regarding security, and also for reporting suspected security breaches or fraudulent behaviour, call centre staff are available to assist clients by email at support@paymont.eu or by telephone at +370 627 51 117, who will provide assistance or advice on information security or arrange for assistance from PAYMONT's security manager.

In the event that acute new threats are identified, the PAYMONT Security Manager

3. Uživatelská podpora

V případě, že má klient jakýchkoli dotazy ohledně bezpečnosti nebo v případě, že hodlá nahlásit podezření na narušení bezpečnosti nebo na podvodné jednání, jsou klientům k dispozici pracovníci call centra na e-mailu support@paymont.eu nebo na telefonu +370 627 51 117. Tito pracovníci poskytují asistenci nebo rady v oblasti bezpečnosti informací, případně zajistí součinnost

alerts clients via the Internet Banking portal of the danger and the appropriate measures.	bezpečnostního manažera PAYMONT. V případě, že jsou identifikovány akutní nové hrozby, bezpečnostní manažer PAYMONT prostřednictvím portálu internetového bankovnictví upozorní klienty na nebezpečí a na vhodná opatření.