Frank Digital AG

SECURITY RISKS

Client’s cryptocurrency wallet/account and email account(s) safety.

The Client must take all reasonable steps to keep Client’s cryptocurrency wallet/account, password and any other security features safe at all times and never disclose them to anyone.

The Client must take all reasonable care to ensure that the Client’s email account(s) are secure and only accessed by the Client, as the Client’s email address may be used to receive security codes, which is used for funds withdrawal from the Client’s cryptocurrency wallet/account, to reset passwords or to communicate with the Client about the security of your cryptocurrency wallet/account. In case any of the Client’s email addresses registered with Frank Digital become compromised, The Client should without undue delay after becoming aware of this event, contact Frank Digital and also contact the Client’s email service provider.

Our personnel will never ask you to provide your email password and any other email security features (e.g., OTP, 2FA etc.) to us or to a third party. The Client must manage and use his/her email privately and con1dentially without granting any access to anyone, including by means of remote-control services (VPN, the same device usage, TeamViewer, etc.).

Any message the Client receives or website visits that asks for the Client’s password or other security features should be reported to Frank Digital. If the Client is in doubt whether a website is genuine, the Client should contact Frank Digital. It is advisable to the Client to change password regularly, i.e., at least every three months, in order to reduce the risk of a security breach in relation to the Client’s cryptocurrency wallet/account. Frank Digital also advises the Client not to choose a password that is easily guessed from information someone might know or gather about the Client or a password that has a meaning.

Irrespective of whether the Client is using a public, a shared or his/her own computer to access his/her email and/or cryptocurrency wallet/account, the Client must always ensure his/her login details are not stored by the browser or cached or otherwise recorded. The Client should never use any functionality that allows login details or passwords to be stored by the computer he/she is using.

The Client must comply with the security procedures Frank Digital informs the Client about from time to time.

The Client, not Frank Digital, is responsible for maintaining adequate security and control of any and all IDs, passwords, or any other details that the Client uses to access his/her wallet/account and the services. The Client is solely responsible for unauthorized access to and/or unauthorized use of the Client’s wallet/account and/or email, as well as loss, theft, misappropriation and/or exposure to abuse. The Client shall be exclusively liable for all losses and expenses (fully and totally, without any limits, limitations and exclusions) relating to any unauthorized use of the Client’s cryptocurrency wallet/account and/or email account(s), as well as in case(s) where the Client acts fraudulently and/or fails to ful1ll one or more of its obligations relating to correct and safe usage and safe keeping of the Client's cryptocurrency wallet/account and/or email account(s).

Considering that technologies develop speedily and constantly, and it is impossible now to foresee all possible future ways of obtaining illegal access to the Client's cryptocurrency wallet/account and/or email account(s), it is impossible to list all measures that the Client shall take or avoid to ensure safe keeping and use of the Client's cryptocurrency wallet/account and/or email account(s). Nevertheless, the Client bears full responsibility for taking all reasonable precautions and security measures to prevent access of unauthorized persons to the Client's cryptocurrency wallet/account and/or email account(s) and their further use thereof.

OUR SECURITY OBLIGATIONS

Frank Digital AG implements robust technical and organizational measures to safeguard client information and digital assets. These include secure encryption, multi-factor authentication, ongoing vulnerability assessments, and infrastructure-level intrusion detection systems. These measures complement client-side security responsibilities outlined in this document.