Security Policy

A). Security Policy General

A.1. This security policy (hereinafter: “Security Policy”) is an integral part of Terms provided by BetOnYourself.io platform and cannot, in any way, be separated from them. By using the Terms you automatically agree with Security Policy.

A.2. If any misalignment between Security Policy and Terms, Terms shall prevail.

B). User’s Responsibility

B.1. The User is solely responsible for the safekeeping of account credentials (username, email, password), and any access keys such as API keys, two step authentication keys or any other credentials used to authorise or authenticate at the Platform.

B.2. You acknowledge that it is your responsibility to protect your credentials and email account against phishing. Neither the Platform nor the Operator assumes nor accepts liability or responsibility for any loss or damage (whether direct or indirect), whatsoever, caused as a result of phishing emails, phishing websites, phishing advertisements or phishing through other channels. You shall promptly report any successful or failed attempts of phishing to the Operator.

B.3. For increased security measures 2FA Identification may become mandatory to login into the Platform and the User understands it may be required to obtain a compatible mobile device to be able to execute login using an application such as Google Authenticator or Authy.

B.4. The Operator may prompt you to change your credentials, if not regularly updated by you, and you are solely responsible to chose such to substantially differ from your other credentials (e.g. not using passwords same as your social media profiles, emails, names or any kind of simplistic terms) and top limit access to your account by keeping them secure and confidential.

B.5. You shall take care that your computer is not compromised and you have to regularly monitor your computer performance, install appropriate antivirus software, avoid installing software from unknown sources, opening email attachments from unknown senders and avoid visiting risky

websites (e.g. pornography, downloads, games, free applications). You are solely responsible to take all security precautions to prevent your computer from being hacked.

B.6. We cannot guarantee that all the information, programs, texts, etc. contained in the Platform are free from the interference by malicious programs such as viruses, trojans, and other kinds of malware, therefore, your login to the Platform or use of any services offered by this Website, download of any program, information and data from the Platform and your use thereof are your personal decisions and you shall bear any and all risks and losses that may possibly arise therefrom.

B.7. You shall immediately inform the Operator if you suspect any unauthorized use of our account or if your account credentials are compromised, lost or stolen.

B.8. You are liable to observe the security and authentication and any procedures whilst using services of the Platform and timely inform the Operator or any suspicious activities or observations.

B.9. You shall immediately inform the Operator if you suspect any violations to the security rules. The Operator may provide you with instructions how, even not being logged into the Platform, to initiate a temporary freeze of your account. The Operator may charge you for temporary freeze or unlocking of your account on your request.

B.10. If the Operator detects any suspicious activity related to your Account, the Operator may, request additional information from you, including verifying identification, or temporary freeze transactions and logins until a review is conducted; in any way, the Operator is not obligated or required to do so and it is subject to its sole discretion. The Operator shall not be liable nor responsible for any loss incurred by the User as a consequence of conducting security measures.

B.11. You shall log out from the Platform after any use from a shared computer by taking proper steps at the end of session, such as pressing logout and terminating internet browser session.

B.12. You shall not use any device, software or subroutine to intervene or attempt to intervene the normal operation of the Platform.

B.13. You shall not adopt any action that will induce unreasonable size of data loading on the network equipments of the Operator.

B.14. As required to maintain system consistency intact, as well as general order and security of transactions on the Platform, the Operator reserves the right to close relevant orders and take other actions in case of any suspicion of malicious sale or purchase or any other events disturbing the

normal order of transaction of the market as well as unilaterally determine whether you have violated any of the covenants mentioned before and, according to such unilateral determination, apply relevant rules and take actions thereunder and temporary or permanently terminate services to you, without your consent or prior notice to you. Any loss or costs arising from such actions shall be solely borne by the user.

C). Responsible disclosure policy

C.1. Responsible disclosure is a model that provides the Operator with a reasonable amount of time to fix the issue before publishing it elsewhere, not leaking or destroying any User data, not defrauding other Users or the Operator itself in the process of discovery.

C.2. In order to encourage responsible disclosure, we promise not to bring legal action against researchers who point out a problem, provided they do their best to follow the above guidelines.

C.3. Rewards may be paid out to the account of researchers who report previously unknown security vulnerability of sufficient severity. There is no minimum or maximum reward, and we may award higher amounts based on severity or creativity of the vulnerability found.

C.4. The Operator reserves the right to decide if the bug is real and serious enough for the researcher to receive the bounty. As a framework for reference, please consider the following list of things we want to know about: XSS, CSRF, authentication bypass or privilege escalation, remote code execution, obtaining sensitive User information, accounting errors, unjust enrichment via a software issue; and the following are not of interest to us: denial of service, spamming, rate limiting on login or password recovery forms, misconfigured SPF, DKIM or DMARC records, vulnerabilities in software not hosted or not operated by the Operator.

C.5. You can disclose a vulnerability by contacting us directly to email at support@betonyourself.io and please include: code which reproduces the issue, detailed description and potential impact of your bug along with your username for potential pay-out.

BetOnYourself d.o.o., Dunajska cesta 156 – WTC, 1000 Ljubljana, Slovenia, 25.09.2018