SECURITY ADVICE

- Access to services through this Website (or Mobile App) will require the use of a valid username and a password ("**Login Details**") to gain access to or use the services, including any temporary or one-time passwords ("OTP") , if applicable.
- You must take all reasonable steps to keep safe and prevent fraudulent or unauthorised use of your device and the **Login Details**. These precautions, include to the extent applicable:
    - to immediately destroy any original printed copy of the **Login Details** received from OnePlatform;
    - not to set a password that is easy to guess (e.g. not to include information such as your birthday, telephone number or a recognizable part of your name) and not to use the same password to access any other services;
    - to keep, at all times, the **Login Details** secret and not to disclose to, share with, allow access to or use by any unauthorised person;
    - not to write down or record the **Login Details** in a manner that could result in its disclosure to or misuse by any other person or otherwise permit any other person to gain access to the Account through this Website (or Mobile App) (e.g. on the mobile device);
    - to change any passwords on a regular basis;
    - to act in such manner so as to avoid "shoulder surfing" of the **Login Details**;
    - not to use public or shared computer systems or public Wi-Fi to access the services and/or this Website (or Mobile App);
    - if we send an OTP to your mobile device, not to send or forward this OTP from one mobile device to another, and not to allow the OTP to come into the possession or control of any unauthorised persons;
    - install the appropriate anti-virus, personal firewall software and other security software to protect the device that you use to access the services;
    - safeguard against social engineering techniques for obtaining your information such as the **Login Details** through fake or suspicious emails, websites or internet banking Website locations or impersonation of OnePlatform's staff or the police;

- not to download any software or application from or access any website of mistrusted sources;
- to prevent any unauthorized access to the Service, this Website (or Mobile App) and/or the relevant mobile device;
- must inform OnePlatform as soon as reasonably practicable after you find or believe that
  (i) the **Login Details** have been misused or compromised; (ii) there has been unauthorized access to the service through this Website (or Mobile App); or (iii) unauthorized transactions or dealings have been conducted through the Account(s); and
- promptly check any confirmation advice or statement received from OnePlatform, including any information about the date and time of the last login to this Website (or Mobile App), and to notify OnePlatform as soon as practicable by contacting OnePlatform's staff through designated means as posted by OnePlatform in this Website (or Mobile App), whenever unauthorised or unusual transactions or observations are detected.