Part C - Additional Security Terms applicable to use of our API

1. **About this Part**

This Part C applies to all Customers and Resellers who use our API for integrations, including integrations with the Customer's or Reseller's systems or other applications and/or to build integrations ("**Integrations**").

2. **Information Security**

(a) In relation to your use of our API in Integrations, without limiting any other obligation you have under your Customer Contract and/or Reseller arrangement, you agree as follows:
   i. you will implement and maintain in place appropriate administrative, physical, and technical data security safeguards and controls, in accordance with best industry standards, that are designed to prevent unauthorised access, use, processing, storage, destruction, loss, alteration, disclosure of Personal Information and other sensitive data and confidential information;
   ii. you will comply with all applicable Laws (including Data Protection Legislation);
   iii. you will keep all credentials that we issue to you strictly confidential and not disclose them to any third party;
   iv. if you become aware of any data breach or other security deficiency or we notify you of any such breach or deficiency, you will:
      (A) follow our reasonable instructions to immediately correct any security deficiency, and will immediately disconnect any intrusions or intruders; and
      (B) not release any public statements (including, without limitation, any press release, blog post or social media) without our prior written approval to the proposed statement.

(b) We do not accept responsibility or liability for any loss or damage arising from your failure to maintain the security of your Integration or login, password or other security or identification credentials.

(c) You agree that we may monitor use of our API in your Integrations to ensure quality, improve our products and services, identify security issues and verify your compliance with this Part C, which may include us accessing and using your Integration and associated applications for any of the foregoing purposes. You agree not to interfere with our monitoring activities and you agree that we may use any technical means to overcome such interference. We may suspend your access to our API without notice if we reasonably believe that you are in violation of any provision of this Part C.

(d) You agree not to use our API in any Integrations that run applications on our servers.

(e) Your networks, operating system and software of your web servers, routers, databases, and computer systems (collectively, "**Developer System**") must be properly configured to Internet industry standards so as to securely operate the application(s) associated with use of our API and protect against unauthorised access to, disclosure or use of any information you receive from us. If you do not completely control any aspect of the Developer System, you will use all practicable measures to procure compliance with this Part C by any relevant third party. You must correct any security deficiency as soon as practicable and disconnect immediately any known or suspected intrusions or intruder.

3. **API Use Restrictions**

(a) When using our API, you will, and you will ensure that your employees, agents and service providers will:
   i. only use our API (including software development kits) to develop and distribute applications or content for your use with the Services;
   ii. restrict disclosure of the API credentials, or any part thereof, to your agents, employees, or services providers, who must require access to use, maintain, implement, correct or update your application in accordance with this Part C, and who

are subject to confidentiality obligations the same as or greater than those contained in your Customer Contract;

iii. not distribute, sell, lease, rent, lend, transfer, assign or sublicense any rights granted in relation to our API to any third party;

iv. not use or access our API or a Service in order to monitor the availability, performance, or functionality of our API or any Service or for any similar benchmarking purposes;

v. not remove or destroy any copyright notices, proprietary markings or confidentiality notices placed upon, contained within or associated with our API;

vi. not engage in any activity that interferes with, disrupts, harms, damages, or accesses in an unauthorized manner our servers, security, networks, data, applications or our other properties or services or those of any third party;

vii. not circumvent technological measures intended to prevent direct database access, or manufacture tools or products to that effect;

viii. not modify, translate, reverse engineer, disassemble, reconstruct, decompile, copy, or create derivative works of our API or any Service, except to the extent that this restriction is expressly prohibited by applicable law;

ix. not bypass our API restrictions for any reason, including automating administrative functions;

x. not, except as authorised by us in writing, substantially replicate our API, a Service or our other products or services or those of any of our Related Bodies Corporate;

xi. not develop applications that excessively burden our system, distribute spyware, adware or other commonly objectionable programs;

xii. not develop an application that has the purpose of migrating our customers off our Services;

xiii. not access or use our API to develop or distribute your application in any way in furtherance of criminal, fraudulent, or other unlawful activity, or otherwise violate the our Acceptable Use Policy;

xiv. not request more than the minimum amount of data from our API needed by your application to provide the intended functionality of such application, or any data outside any permissions granted by a relevant third party merchant;

xv. not falsify or alter any unique identifier in, or assigned to your application, or otherwise obscure or alter the source of queries coming from such application; and

xvi. not include code in any of your applications which performs any operations not related to the services provided by the application, whether or not you have the consent of any relevant merchant or end user to do so. For the avoidance of doubt, this prohibited activity includes, without limitation, embedding or incorporating code into any application which utilises the resources of another computer for the purposes of cryptocurrency mining.