SecureWeb3.io
Special Services Terms (SSTs)
Brand Protection Platform (Self-Service)

These Special Services Terms (**SSTs**) SSTs apply to your self-directed use of SecureWeb3 Brand Protection Platform (the **Service**) and are entered between the individual or business entity (**Company**, **you**, or **your**) that engages with, uses, accesses, or otherwise receives (**Receives**, **Receiving**, or **Receipt**) the Service, and SecureWeb3 Ltd, a limited company registered in the United Kingdom under company number 14593990 (**SecureWeb3**, **we**, **our**, or **us**).

These SSTs, as amended from time to time, together with the General Services Terms (**General Terms**) and each of the policies or terms incorporated into the General Terms including the Privacy Notice (hereinafter collectively referred to as the **Agreement**) shall govern your Receipt of the Service. <u>If you do not agree with any of the terms contained in the Agreement, you should not Receive or purchase the Service.</u>

In the event of any inconsistency between the terms included herein and those included in the General Terms, the terms and conditions of these SSTs shall prevail to the extent of such inconsistency. By Receiving the Service, you agree to the terms contained herein.

<u>Interpretation</u>	**1. Definitions**
	1.1. In these SSTs:
	Applicable Blockchains means the specific blockchain networks monitored by the Platform as may be updated from time to time;
	Authorised User means any individual who is a Representative of the Company and who is authorised by the Company to access Platform and Receive the Service;
	Associated Web3 Wallet means, collectively, the SW3 Wallet and any External Wallet embedded in the Platform for the benefit of Company;
	Core Functions means the core functionalities of the Platform including Monitoring Features, Alerts, and Enforcement Features, as more particularly described in these SSTs;
	Enforcement Features means the Intellectual Property enforcement and protection features of the Platform, as more particularly described in these SSTs;
	External Wallet means any Web3 Wallet address that is added to Company's Account for the purposes of receiving a Web3 Domain purchased in accordance with paragraph 4.21;
	Initial Services Term means the initial duration the Company will receive the Service and access to the Platform as selected in the Onboarding Process and subject to automatic renewal as set out in the General Terms;
	Infringing Wallet means the Web3 Wallet address identified by the Platform and confirmed by Company as a Potential Infringement;
	License means the personal license granted by SecureWeb3 to Company to access, use, and exploit the Platform for its own internal business usage pursuant to the License terms provided under paragraph 5;
	Monitoring Functions means the continuous scanning of the Applicable Blockchains for instances of Potential Infringement;
	NFT means Non-Fungible Token;
	Platform means SecureWeb3 Brand Protection Platform;
	Potential Infringement means the potential third party infringement of Company's IPR in the Company Assets as identified by the Monitoring Functions and confirmed by the Company;
	Service means the Licence granted to Company in the Platform and any other related or ancillary services provided by SecureWeb3 in accordance with these SSTs;

	SW3 Wallet means the Web3 Wallet address that is created by SecureWeb3 for Company's use when Receiving the Service, including for the purchase of any Web3 Domains;

Takedown Request means the request initiated by Company through the Platform, to send a takedown request or other legal demand to an Infringing Wallet;

Token means a digital representation of value that operates within one of the Applicable Blockchains known as a 'fungible' or native token, but not including NFTs;

User Details means the username, password and any other access credentials of an Authorised User;

Web3 Domain means a name registered and resolved on a blockchain network, such as .eth or .crypto that can be used for purposes such as sending or receiving Tokens or NFTs;

Web3 Domain Provider means an entity who offers Web3 Domains for purchase via the Platform on the Applicable Blockchains; and

Web3 Wallet means a software application that allows users to store, manage, and use their blockchain-based assets, such as Tokens, NFTs, or Web3 Domains. |
| <u>Services Term; Termination</u> | **2. Services Term**

Commencement & Duration

2.1. The Service will commence on the date SecureWeb3 receives the Fees for the Initial Services Term (**Service Commencement Date**), and will continue for the Initial Services Term, unless terminated earlier in accordance with the Agreement.

2.2. Upon expiry of the Initial Services Term, the Service will automatically renew for successive periods equal to the Initial Services Term (each a **Renewal Term**), unless either party provides written notice of its intention not to renew at least thirty (30) days before the end of the then-current Initial Services Term or Renewal Term (as the case may be).

2.3. SecureWeb3 reserves the right to modify the Fees for any Renewal Term by providing written notice to Company not less than forty-five (45) days prior to the commencement of the Renewal Term. If Company does not agree to such modified Fees, it may cancel the Service in accordance with paragraph 2.2 above.

Service Cancellation

2.4. The Service may be cancelled in accordance with the provisions of the General Terms. This right to cancel is in addition, and without prejudice, to the right not to renew set forth above at paragraph 2.2

2.5. Upon termination or expiration of the Services Term, Company's access to the Platform will be discontinued or limited at the end of the then-current Services Term. |
| <u>Users & Accounts</u> | **3. Users & Accounts**

Onboarding Process

3.1. To access our Platform you must register an Account and provide us with certain information about you (as a user of the Platform) and the Company. We will handle all information you provide to us when registering an Account with us in accordance with our Privacy Notice.

3.2. When registering an Account, you represent and warrant that:

    (a)   you are legally authorised to do so on behalf of the Company;

    (b)   you will only provide accurate, complete and current information about the Company and any authorised personnel of the Company who may access the Platform;

    (c)   you intend to use the Service for internal business usage only; |

(d)   you will comply with the Agreement and any reasonable instructions given by SecureWeb3 from time to time.

3.3.   SecureWeb3 reserves the right to deactivate any Account or suspend any Authorised User if it reasonably believes the above warranties have not been complied with and may do so without notice.

Authorised Users

3.4.   You may grant access to the Platform to certain Authorised Users on behalf of the Company subject to any limitations set out in the Agreement (including these SSTs) or as otherwise notified by SecureWeb3. You are responsible for ensuring that each Authorised User:

(a)   is legally able to access the Platform without breaching any applicable laws;

(b)   keeps their User Details confidential, safe and secure at all times;

(c)   does not share, disclose, provide access, or otherwise make available their User Details to any person, including other Representative of the Company; and

(d)   uses the Platform and Services in accordance with the Agreement and any reasonable instructions given by SecureWeb3 from time to time.

3.5.   You are, and will be held responsible for, all actions, activities and transactions that occur under your Account, whether they are made by an Authorised User or otherwise.

3.6.   You agree to:

(a)   notify us if any of your Account information is outdated or incorrect;

(b)   notify us if you have reason to believe that a person other than an Authorised User has accessed, or has access to, your Account; and

(c)   only use, or permit the use of, your Account for the purposes for which it is intended and licensed.

3.7.   You may request the deletion of your Account at any time by contacting us.

Service Description	**4. Service Description**

Core Functions; Self-Use

4.1.   The Platform offers a comprehensive suite of features and functionalities designed to help you and your businesses safeguard your brand and Company Assets. While we continually update and improve the Platform's functionalities (which we reserve the right to do), the Core Functions include: (i) monitoring; (ii) reporting and alerts, and; (iii) Intellectual Property protection and enforcement.

4.2.   As a self-service customer, you shall be wholly responsible for determining how the Core Functions are utilised, including their frequency and application. You affirm that your use of the Core Functions will be in strict adherence to the terms of this Agreement and applicable laws, and any reasonable instructions given to you by SecureWeb3 from time to time.

4.3.   These SSTs do not apply to any customer who receives the Services on a managed basis. If SecureWeb3 performs the functions and features of the Platform on your behalf, please refer to the Managed Services SSTs.

Monitoring Features

4.4.   The Platform actively monitors the Applicable Blockchains for instances of Potential Infringement potential (**Monitoring Features**). At the date of these SSTs, the Applicable Blockchains include Ethereum, Polygon, and Solana however these are subject to change at any time. Whilst we will inform you in writing if we choose to

remove any of the Applicable Blockchains, we reserve the right (and intend to) add additional blockchain networks to our capabilities and may do so without notice.

4.5. Our monitoring process involves the continuous download and organisation of blockchain data from the Applicable Blockchains. The Platform scans for Potential Infringement across various Web3 technologies, including, Fungible Tokens and Non-Fungible (NFT's) including Web3 Domains (collectively, **Monitored Assets**).

4.6. We reserve the right to modify, enhance, or expand any of our monitoring capabilities, including the suite of Monitored Assets and agree to notify you in writing in the event of Service degradation or removal of a Monitored Asset.

Alerts and Reporting

4.7. For any newly registered Monitored Asset on the Applicable Blockchains that appear to be a Potential Infringement, the Platform will provide Company's Authorised User(s) with a real-time email notification (**Alert**) which can be managed via the Platform's settings. SecureWeb3 will not be liable for any Alert which is not viewed, accessed, received, or otherwise actioned by such Authorised User in a timely manner, including any Alerts which are delivered to the Authorised User's junk or spam email folders.

4.8. The Platform also offers the capability to download Reports and associated data in readable format. Authorised Users can request Reports based on activities associated with the Monitoring Features and Enforcement Features of the Platform, as undertaken by Company.

Protection & Enforcement

4.9. The Platform offers several protection & enforcement features which allow you to further protect your IPR in the Company Assets (**Enforcement Features**). The Enforcement Features include:

(a) the facilitation of a streamlined complaint process with the concerned Web3 Domain registrar or NFT marketplace or Blockchain Explorer where the Potential Infringement can be viewed;

(b) the ability to initiate and transfer a Takedown Request directly to an Infringing Wallet; and

(c) assistance with the engagement of formal legal representation.

4.10. When you initiate a Takedown Request, we will, using blockchain technology:

(a) create an NFT on your behalf in relation to the Takedown Request;

(b) subject to paragraph 4.12(c), include within the Takedown Request such content as may be provided by the Authorised User when requesting the Takedown Request;

(c) facilitate and execute the transfer of the NFT to the Infringing Wallet on the Applicable Blockchain; and

(d) include, within the NFT description, any disclaimer in which SecureWeb3 deems as appropriate.

4.11. Whenever you initiate a Takedown Request, you hereby appoint SecureWeb3 to facilitate the transfer of the Takedown Request on the Company's behalf. Company acknowledges that SecureWeb3 is and acts as a technology facilitator only and will not be held responsible nor liable for the Takedown Request's contents or Service Output,

4.12. In respect of a Takedown Request, Company agrees, undertakes, and warrants to:

(a) upon request, provide written confirmation that SecureWeb3 is authorised to transfer the Takedown Request to the Infringing Wallet;

(b) only initiate a Takedown Request if it reasonably believes that the user of the Infringing Wallet is misappropriating the Company's IPR in the Company Assets;

(c)   not include, or request SecureWeb3 to include, any illicit, defamatory, misleading, derogatory or untrue information in the contents of the Takedown Request; and

(d)   take any action, nor hold SecureWeb3 responsible or liable, for the consequences or outcome of the Takedown Request.

4.13.   Company agrees to remain wholly responsible and liable for the outcome, consequences and other Service Outcome of initiating a Takedown Request and further acknowledges that once a Takedown Request is initiated, it is irreversible given the nature of blockchain technology.

4.14.   Company acknowledges that SecureWeb3 is a technology service provider only and in no way purports, or intends to purport itself, as a provider of legal services. Further, and to the maximum extent allowable under applicable law, SecureWeb3 disclaims all liability in respect of any Takedown Request initiated by the Company and provides no warranties as to its performance or fitness for a particular purpose.

Web3 Wallet Generation

4.15.   Upon registration of an Account, we will procure a Web3 Wallet from our authorised partners which will be embedded within the Platform. The SW3 Wallet is designed to allow Company to store any purchased Web3 Domains when seeking to protect Company's brand and secure available Web3 Domains in relation to the Company Assets. If so desired, the SW3 Wallet may also hold any other compatible digital assets that are compatible with the Applicable Blockchain hosting the SW3 Wallet.

4.16.   Company may also choose to add their own External Wallet within the Platform to perform the activities contemplated under paragraph 4.15. Any External Wallet will be supplementary to, and not in replacement of, the SW3 Wallet.

4.17.   There are no additional Fees payable to SecureWeb3 with respect to any Associated Web3 Wallet.

4.18.   In respect of any Associated Web3 Wallet, each party acknowledges and agrees that Company shall be the beneficial owner of all contents contained within an Associated Web3 Wallet.

4.19.   Company agrees:

(a)   to comply with all applicable laws related to the use of Web3 Wallets;

(b)   that SecureWeb3 will neither be the custodial owner nor have any control, responsibility, or liability in respect of such External Wallet;

(c)   to only use an External Wallet for the purposes intended pursuant to these SSTs;

(d)   to maintain the security and confidentiality of any private keys, seed phrases, or other access credentials;

(e)   comply with any third-party terms associated with an External Wallet;

(f)   comply with any third-party terms notified by SecureWeb3 in respect of an SW3 Wallet;

(g)   immediately notify SecureWeb3 of any suspected or actual unauthorised access or security breach in relation to the External Wallet; and

(h)   not use the External Wallet(s) for any illegal activity, money laundering, or financing of terrorism activities.

4.20.   Company acknowledges that blockchain transactions are irreversible and that Company bears full responsibility for any transactions initiated through an Associated Web3 Wallet. Company further agrees to indemnify and hold SecureWeb3 harmless from any claims, damages, or liabilities arising from Company's use of an Associated Web3 Wallet except in cases of gross negligence or wilful misconduct by SecureWeb3

or if such claim is a result of any instruction made by SecureWeb3 in respect of such Associated Web3 Wallet.

Web3 Domains

4.21. An additional feature of the Platform is the facilitation and ability of an Authorised User to purchase available Web3 Domains through SecureWeb3's partner Web3 Domain Providers.

4.22. When purchasing a Web3 Domain via the Platform, SecureWeb3 will, subject to the Web3 Domain Provider providing the Web3 Domain:

(a) redirect the Authorised User to the official website of the Web3 Domain Provider for Company to continue with the purchase transaction; or

(b) facilitate the purchase of the Web3 Domain from the Web3 Domain provider on behalf of Company directly via the Platform.

4.23. If Company chooses to purchase a Web3 Domain and the circumstances contemplated in paragraph 4.22(b) apply, Company authorises SecureWeb3 to:

(a) act as Company's agent with respect of the Web3 Domain Provider;

(b) upon the confirmation of Company, purchase the applicable Web3 Domain on behalf of the Company;

(c) transfer the Web3 Domain to Company's chosen Associated Web3 Wallet; and

(d) facilitate the payment to the Web3 Domain Provider.

4.24. If paragraph 4.23 applies, Company agrees:

(a) to adhere to any terms associated with the use of the Web3 Domain as may be displayed or otherwise informed to Company prior to such purchase;

(b) that SecureWeb3 acts solely as an intermediary and is not the seller or provider of the Web3 Domain. SecureWeb3 further does not endorse nor assume any responsibility of the Web3 Domain;

(c) that SecureWeb3 shall not be liable for any loss or damage arising from the purchase or use of the Web3 Domain;

(d) to indemnify and hold SecureWeb3 harmless from any claims, damages, or expenses arising from or related to your purchase and use of the Web3 Domain; and

(e) SecureWeb3 makes no warranties, express or implied, regarding the Web3 Domain purchased through the Platform.

4.25. When purchasing any Web3 Domain from a Web3 Domain Provider, Company agrees:

(f) to comply with the relevant policies and procedures of the Web3 Domain Provider;

(g) that the purchase of any Web3 Domain shall be governed by the applicable terms of purchase set by the respective Web3 Domain Provider; and

(h) that it shall be responsible for any transaction made with a Web3 Domain Provider, including the name, hosting blockchain, price and other distinguishing features associated with Web3 Domain

4.26. When purchasing any Web3 Domain from a Web3 Domain Provider, SecureWeb3's role shall be limited to that of a facilitator/intermediary only, and any transaction will be by and between Company and the selected Web3 Domain Provider. SecureWeb3 is in no way responsible for the Web3 Domain Provider's pricing, policies or terms & conditions, responsibility for such being expressly disclaimed.

	4.27. Company expressly acknowledges that the purchase of any Web3 Domain from a Web3 Domain Provider shall be subject to the terms and conditions set by the respective Web3 Domain Provider.
License	**5. Software License** 5.1. In consideration of the payment by the Company of the Fees, SecureWeb3 grants the Company a royalty-free, non-exclusive, worldwide licence to use the Platform on the terms of the Agreement during the Services Term for the purpose of its[internal business requirements in accordance with this paragraph 5. 5.2. The Company shall treat the Platform and all software components underpinning the Platform as confidential and shall not, without the prior written consent of SecureWeb3, disclose the whole or any part of them to any third party. Company shall ensure that its Representatives comply with these confidentiality and non-disclosure obligations. 5.3. The Company shall not alter or modify the whole or any part of the Platform or software components underpinning the Platform nor merge any part of the Platform with any other computer software programs nor, save to the extent expressly permitted by applicable law, decompile, disassemble or reverse engineer the object code of the Platform nor attempt to do any of these things.

Service Fees	**6. Fees**
	
	6.1. All Fees in respect of the Service shall:
	
	(a) be as set out during the onboarding process or as otherwise agreed in advance;
	
	(b) be payable in advance and:
	
	  (i) for any Initial Services Term, upon completion of the Onboarding Process
	
	  (ii) for any Renewal Services Term, upon expiry of the Initial Services Term;
	
	(c) be SecureWeb3's consideration for providing the Service;
	
	(d) including full access to the Core Functions and SW3 Wallet functionality;
	
	(e) not include any fees or charges associated with any Web3 Domain purchased via the Platform;
	
	(f) be subject to change in accordance with paragraph 3.1.2 of the General Terms.
	
	6.2. Notwithstanding and without limiting paragraph 5.1 above, the provisions of Section 3 of the General Terms shall apply to all Service Fees, except to such extent they are inconsistent or conflict with the terms set out in this Section 5 (Fees).

Service Levels	**7. Service Level Agreement** *Service Level Objectives* 7.1. SecureWeb3 will use reasonable endeavours to meet the service level objectives (**SLOs**) set out in this section, which apply to the availability and performance of the Platform. The SLOs are not guarantees and do not constitute a warranty or a condition of the Service or Agreement. 7.2. The Platform will: (a) be available for use by the Company at least 99.5% of the time in any calendar month, excluding scheduled maintenance (**Availability SLO**); and (b) respond to requests from the Company within a reasonable time, taking into account the complexity and volume of the requests, the network conditions, and the load on the Platform (**Performance SLO**).

	7.3. If SecureWeb3 fails to meet an SLO in any calendar month, the Company may request a service credit equal to 1% of the Fee for the Services Term for each percentage point below the SLO, up to a maximum of 10% of the Service Fee (**Service Credit**). 7.4. The Company must request the Service Credit within fifteen (15) days of the end of the month in which the failure occurred, providing sufficient evidence of the failure. The Service Credit will be applied to the next invoice or refunded to the Company, at SecureWeb3's discretion. The Service Credit is the Company's sole and exclusive remedy for any failure to meet an SLO. *Support* 7.5. SecureWeb3 will provide such support services to the Company as may be required for the effective use and functionality of the Platform. 7.6. SecureWeb3 will use reasonable efforts to respond to and resolve the Company's support requests in a timely and professional manner, in the order of requests in which they are received.
Special Terms	**8. Special Terms** *Specific Disclaimer of Warranties* 8.1. SecureWeb3 does not warrant that any Takedown Request or any Service Output, including, without limitation, consequences, or outcomes of a Takedown Request, will meet the Company's requirements, expectations, or objectives, or that they will be effective, successful, or enforceable in any jurisdiction. 8.2. SecureWeb3 is not responsible for any loss or damage caused by third parties, including but not limited to the recipients of the Takedown Requests, the owners or operators of the infringing websites or content, or any other parties involved in the Takedown Request process, or by any events or circumstances beyond its reasonable control, including but not limited to legal disputes, technical issues, or delays. 8.3. SecureWeb3 does not provide any legal services or advice, and the Company is solely responsible for ensuring that its use of the Takedown Request functionality complies with all applicable laws and regulations and does not infringe any rights of any third parties. 8.4. The Company acknowledges and agrees that the Takedown Request service and the Takedown Request output are provided at its own risk and discretion, and that it relies on them solely at its own responsibility.

Addendum No. 1 to Brand Protection Platform (Self-Service)

SecureWeb3 API Access

IMPORTANT: THIS ADDENDUM NO. 1 APPLIES ONLY TO THOSE CUSTOMERS WHO CHOOSE RECEIVE ANY OF SECUREWEB3'S API SERVICES. IF YOU DO NOT INTEND ON PURCHASING OR OTHERWISE RECEIVING SECUREWEB3'S API SERVICES, THIS ADDENDUM NO. 1 DOES NOT APPLY TO YOU.

This Addendum No. 1 to the Brand Protection Platform (Self-Service) SSTs (**Addendum**) applies solely to Company's Receipt of (i) SecureWeb3 API (the **API**); (ii) any API key provided by SecureWeb3 to access the API (**API Key**), and (iii) any access to the repository of organised public blockchain data managed by SecureWeb3 and in which the API relates (**Data Repository**) (collectively, the **API Services**).

By Receiving the API Services, you agree to be bound by the terms of this Addendum. If you do not Receive or otherwise purchase any API Services from SecureWeb3, this Addendum does not apply to you and can be disregarded. <u>If you do not agree with any of the terms contained in the Agreement, including the SSTs or this Addendum, you should not Receive or purchase the API Services.</u>

In the event of any inconsistency between the terms included herein and those included in the SSTs, the terms and conditions of this Addendum shall prevail to the extent of such inconsistency, but only in relation to the API Services. For the avoidance of doubt, all terms in the SSTs not specifically modified by this Addendum remain in full force and effect.

Interpretation	1. Interpretation
	Definitions
	1.1. In this Addendum:
	API means the application programming interface provided by SecureWeb3 that allows Company to access and query the Data Repository;
	API Call means each call from a Company Application via the API to interact with the Data Repository;
	API Fees means the fees payable by Company for Receiving the API Services as set out in the API Module or as otherwise agreed in advance;
	API Key means the unique identifier issued by SecureWeb3 to Company to authenticate and authorise Company's access to the API and Data Repository;
	API Module means user interface module of the Platform relating to the API where Company can purchase, manage and otherwise Receive the API Services, including the API Key;
	API Package Plan means a specific offering of API Services selected by Company via the API Module which defines the scope of the API Services, including, without limitation, the API Usage Limits and API Fees;
	API Renewal Term means any period subsequent to the Initial API Term where Company Receives the API Services, as more particularly described at paragraph 2.2;
	API Term means the Initial API Term and any API Renewal Term(s) as the case may be;
	API Usage Limits means the limits imposed by SecureWeb3 on the usage of the API as more particularly described under paragraph 3.8;
	Authorised Purpose means those purposes of which the API and Licensed Data can be used, as set out in this Addendum or otherwise notified by SecureWeb3;
	Company Application means any applications developed by, or on behalf of, the Company to interact with the API;

	Data Repository means the database of public blockchain data collated from the Applicable Blockchains, organised, maintained, and updated by SecureWeb3 as accessible via the API;
	Initial API Term means the initial period in which Company Receives the API Services, as selected in the API Module;
	Licensed Data means the data extracted from the Data Repository by Company via the API which is not Raw Data; and
	Raw Data means the publicly available data extracted from the Applicable Blockchains before being processed and organised by SecureWeb3 to become Licensed Data.
API Services Term	**2. API Services Term**
	Commencement & Duration
	2.1. The API Services will commence on the date SecureWeb3 provides Company with the API Key and will continue for the Initial API Term, unless terminated earlier in accordance with the Agreement.
	2.2. Upon expiry of the API Term, the API Services will automatically renew for successive periods equal to the Initial API Term (each an **API Renewal Term**), unless either party provides written notice of its intention not to renew at least thirty (30) days before the end of the then-current API Term or Renewal Term (as the case may be).
	2.3. SecureWeb3 reserves the right to modify the API Fees or API Usage Limits for any Renewal Term by providing written notice to Company not less than forty-five (45) days prior to the commencement of the Renewal Term. If Company does not agree to such modified Fees or Usage Limits, it may cancel the API Services in accordance with paragraph 2.4 of this Addendum below.
	2.4. For the avoidance of doubt, the API Term is distinct and separate from the Services Term relating to Company's Receipt of the Platform Services, save that Company must have an active Account to receive the API Services.
	Service Cancellation
	2.5. The API Services may be cancelled in accordance with the provisions of the General Terms. This right to cancel is in addition, and without prejudice, to the right not to renew set forth above at paragraph 2.2 to this Addendum.
	2.6. Upon termination or expiration of the API Term, Company agrees to cease Receiving the API Services and acknowledges that all existing rights to access the Licensed Data or Receive the API Services shall cease.
API Access & Usage	**3. API Access & License**
	API Access
	3.1. To Receive the API Services and receive an API Key,, Company must first select an API Package Plan via the API Module. SecureWeb3 offers a variety of API Package Plans, details of which can be found on the Product Pages or via the API Module.
	3.2. Upon purchasing an API Package Plan and paying the applicable API Fees, SecureWeb3 will issue the Company with an API Key. The Company's sole means of accessing the API shall be via the API Key.
	3.3. To receive an API Key, Company must:
	(a) have an active Account on the Platform;
	(b) purchase an API Package Plan;
	(c) have paid the API Fees for the Initial API Term;

(d) and and be in good standing; and

(e) provide SecureWeb3 with such information as may reasonably be requested via the API Module or otherwise.

3.4. SecureWeb3 reserves the right to deny any request made by Company for the issuance of an API Key.

API Usage

3.5. In consideration of the API Fee paid by Company, SecureWeb3 grants Company a non-exclusive licence for the API Term (including any Renewal Term):

(a) for the Authorised Users to access the API solely for the purposes of:

(i) internally developing and/or operating any Company Applications that will communicate and interoperate with the API and make API Calls to the Data Repository;

(ii) making API Calls in compliance with the API Limits;

(b) to display the API Data received from the API, together with any Licensed Data, within the Application for any Authorised Purpose.

Usage Limits

3.6. Company agrees to only Receive the API Services in accordance with API Usage Limits associated with the API Package Plan purchased by Company. The applicable API Usage Limits will be detailed in the API Package Plan description which is available via the API Module of the Platform.

3.7. Whilst SecureWeb3 reserves the right to update or otherwise amend the API Usage Limits at any time and its discretion, the API Usage Limits may include, without limitation, restrictions on (i) the number of API Calls made by Company each month; (ii) the frequency attempted API Calls, or; (iii) the volume of data transfer requested by Company.

3.8. SecureWeb3 may update or impose additional API Usage Limits for any API Package Plan at any time at its discretion save that any such updates will not come into effect until the expiry of the then Initial API Term or API Renewal Term (as the case may be) pursuant to paragraph 2.3 above.

3.9. If Company exceeds the API Usage Limits associated with its then-current API Package Plan, SecureWeb3 may, at its sole discretion:

(a) charge Company additional API Fees for the excess usage, as notified by SecureWeb3;

(b) require Company to upgrade to a higher API Package Plan;

(c) suspend or limit Company's access to the API Services until the next Renewal Term; or

(d) terminate Company's Receipt of the API Services in accordance with the Agreement

Restrictions	**4. Restrictions** *API Restrictions* 4.1. In relation to the scope of use set out in paragraph 3.3, the Company shall not: (a) make API Calls in excess of the API Limits; (b) use the API or Licensed Data in any manner or for any purpose that infringes, misappropriates, or otherwise infringes any third party rights (including Intellectual Property Rights) or that violates any applicable law;

<table>
<tr><td></td><td>

(c)   design or permit any Company Application to disable, override, or otherwise interfere with any SecureWeb3-implemented technology;

(d)   use the API, including in any Company Application, to replicate or attempt to replace the user experience of the Platform;

(e)   attempt to cloak or conceal the Company's identity or the identity of the Company Application when requesting authorisation to use the API or making an API Call;

(f)   except to the extent expressly permitted under this Addendum or with SecureWeb3's prior written consent:

     (i)   combine or integrate the API or Licensed Data with any software, technology, services, or materials not approved in advance by SecureWeb3, including AI-related technologies, large language or other foundation models;

     (ii)   pass or allow access to the API or Licensed Data to any third party; or

     (iii)   access all or any part of any the API or Licensed Data to build a product and/or service which competes with the API, the Platform, or any other services provided by SecureWeb3.

(g)   interfere with or disrupt the operation or performance of the API, the Data Repository, or the Platform, or any networks or systems connected to them.

(h)   attempt to circumvent, bypass, or breach any security, authentication, or verification measures implemented by SecureWeb3 in relation to the API, the Data Repository, or the Platform.

4.2.   Except as expressly stated in this Addendum, the Company has no right (and shall not permit any third party) to copy, adapt, reverse engineer, decompile, disassemble, modify, adapt, or make error corrections to the API, in whole or in part.

4.3.   Without prejudice to its other rights and remedies under this Agreement, should the Company use the API or Licensed Data other than as specified in this Addendum without the prior written consent of SecureWeb3, SecureWeb3 may, in its sole discretion, terminate or suspend the Company's Receipt of the API Services or Licensed Data without notice.

</td></tr>
<tr><td>

API Fees

</td><td>

5.   API Fees

API Fees

5.1.   Company shall pay SecureWeb3 the API Fees for Receiving the API Services as set out in the Platform's API Module or as otherwise agreed in advance.

5.2.   The API Fees shall be payable in advance and:

   (a)   for any API Term, upon completion of the API Key request; and

   (b)   for any Renewal Term, upon expiry of the API Term.

5.3.   The API Fees shall be subject to change in accordance with paragraph 2.3 of this Addendum.

5.4.   The provisions of Section 3 of the General Terms shall apply to all API Fees, except to such extent they are inconsistent or conflict with the terms set out in this Addendum.

</td></tr>
<tr><td>

Data Ownership and License

</td><td>

6.   Data Ownership and License

Data Ownership

</td></tr>
</table>

	6.1. SecureWeb3 does not claim ownership or rights over the Raw Data, which is publicly available data extracted from the Applicable Blockchains before being processed and organised by SecureWeb3.
	6.2. SecureWeb3 retains all rights, title, and interest in and to the API, the Licensed Data, and any data, information, or content derived or generated from them. This includes any modifications, enhancements, or improvements made by SecureWeb3 or any third parties.
	6.3. Company owns and retains all rights, title, and interest in and to any data, information, or content that it provides to SecureWeb3 via the API or the Platform (including any Company Data), subject to SecureWeb3's right to use such data, information, or content for the purposes of providing the API Services and the Platform, and for its own internal business purposes, in accordance with the Agreement and the Privacy Notice.
	Data License
	6.4. SecureWeb3 grants the Company a limited, non-exclusive, non-transferable, revocable license to access and use the API and the Licensed Data for its internal business purposes only during the API Term.
	6.5. The Company cannot sublicense, assign, transfer, or otherwise grant any rights in or to the API or Licensed Data to any third party without SecureWeb3's prior written consent.
	6.6. The Company must acknowledge and attribute SecureWeb3 as the source of the API and Licensed Data in any publications, presentations, or reports that incorporate or reference them in a manner reasonably acceptable to SecureWeb3.
Special Terms	**7. Special Terms**
	Specific Disclaimer of Warranties
	7.1. SecureWeb3 does not warrant that the API Services, including any Licensed Data accessed through the API, will meet the Company's requirements, expectations, or objectives, or that they will be uninterrupted, error-free, or secure. The Company acknowledges and agrees that the API Services are provided on an 'as-is' and 'as-available' basis, and that it uses the API Services at its own risk and discretion.

LAST UPDATED ON 31 AUGUST 2024