Doc. name : **Oxygis - Acceptable Use Policy**

Version : 18/06/2025

Summary: Use of Oxygis cloud services is subject to this Acceptable Use Policy (AUP). This AUP is incorporated by reference into and governed by the ***Oxygis Subscription Agreement*** between you (Client) and Oxygis Partners SRL. Clients who violate these rules may have their subscription **suspended without notice**. Subscription fees will generally **not** be refunded.

I. Illegal or harmful use

You may not use the Oxygis Cloud Services to store, display, distribute or otherwise deal with illegal or harmful content. This includes:

- **Illegal activities:** promotion of sites or services linked to gambling or child pornography.
- **Harmful or fraudulent activities:** Activities harmful to others, promotion of fraudulent goods, services, schemes or promotions (for example, get-rich-quick schemes, Ponzi and pyramid schemes, phishing or pharming), or other deceptive practices.
- **Illegal content:** Content that infringes the intellectual property rights of others.
- **Offensive content :** Content that is defamatory, obscene, abusive, invasive of privacy or otherwise objectionable, including content that constitutes child pornography, relates to bestiality or depicts non-consensual sexual acts.
- **Harmful content:** Malicious and malware content, such as viruses, Trojan horses, worms, etc.
- **Spam Content:** Content published for "black hat SEO" purposes, using tricks such as link building / link spam, keyword spam, in order to exploit the reputation of Oxygis services to promote third-party content, goods or services.

The Client remains solely responsible for the compliance of data hosted or processed via Oxygis Cloud services with applicable laws and regulations, in particular the General Data Protection Regulation (GDPR).

II.Safety violations

You may not attempt to compromise Oxygis Cloud services, access or modify content that does not belong to you, or engage in other malicious actions:

- **Unauthorized access:** unauthorized access to or use of any Oxygis Cloud system or service.
- **Security Research:** Conduct any security research or audit on Oxygis Cloud systems without written permission, including via scanners and automated tools. Please see our ***Responsible Disclosure*** document for more information on Oxygis security research.
- **Listening:** listening to or recording data that does not belong to you without authorisation.
- **Other attacks:** non-technical attacks such as social engineering, phishing or physical attacks against any person or system.

III.Abuse of networks and services

You must not abuse the resources and systems of Oxygis Cloud. In particular, the following activities are prohibited:

- **Network abuse:** causing a denial of service (DoS) by flooding systems with network traffic that slows down the system, makes it inaccessible or has a significant impact on the quality of service.
- **Unthrottled RPC/API calls**: sending a large number of remote RPC or API calls to our systems without appropriate throttling, with the risk of impacting the quality of service for other users. Note: Oxygis provides batch APIs for imports, which should not be necessary. Limited calls are generally acceptable for non-sustained use, at a rate of one call per second, with no parallel calls. Exceptions may be allowed on a case-by-case basis for Oxygis Cloud (please **contact us** if you feel you need this), dedicated hosting mode may be considered as an alternative to this restriction.
  Any automation (including the use of bots, scripts or external integrations) interacting with the Software or its APIs must remain reasonable, documented and in accordance with best practices. Oxygis reserves the right to restrict or block any automated behavior that disrupts the stability or security of the platform.
- **Overload**: deliberate impact on the performance or availability of systems with abnormal content such as very large quantities of data, or a very large number of items to be processed, such as electronic bombs.
- **Crawling:** automatic exploration of resources in a way that has an impact on system availability and performance.
- **Attack:** using Oxygis Cloud services to attack, crawl or otherwise impact the availability or security of third-party systems.
- **Abusive registrations:** use of automated tools to repeatedly register or subscribe to Oxygis services.

IV.Consequences in the event of a breach

In the event of non-compliance with this policy, Oxygis reserves the right to suspend or restrict the Client's access to its Services. Where possible, prior notification will be sent to allow the Client to rectify the situation. In the event of a serious, intentional or repeated breach, Oxygis reserves the right to suspend access immediately, without refund.