Nom doc. :	**Oxygis - Politique d'Utilisation Acceptable**
Version :	18/06/2025
Résumé :	L'utilisation des services cloud d'Oxygis est soumise à la présente Politique d'Utilisation Acceptable (PUA). La présente PUA est incorporée par référence dans le ***contrat d'abonnement Oxygis*** entre vous (Client) et Oxygis Partners SRL et est régie par celui-ci. Les Clients qui enfreignent ces règles peuvent voir leur abonnement **suspendu sans préavis**. Les frais d'abonnement ne seront généralement **pas** remboursés.

I. Utilisation illégale ou nuisible

Vous ne pouvez pas utiliser les services Oxygis Cloud pour stocker, afficher, distribuer ou traiter de toute autre manière du contenu illégal ou nuisible. Cela inclut :

- **Activités illégales :** promotion de sites ou de services liés aux jeux d'argent ou à la pornographie enfantine.
- **Activités nuisibles ou frauduleuses :** Activités préjudiciables à autrui, promotion de biens, de services, de systèmes ou de promotions frauduleux (par exemple, systèmes permettant de gagner de l'argent rapidement, systèmes de Ponzi et pyramidaux, phishing ou pharming), ou autres pratiques trompeuses.
- **Contenu illicite :** Contenu qui porte atteinte à la propriété intellectuelle d'autrui.
- **Contenu offensant :** Contenu diffamatoire, obscène, abusif, portant atteinte à la vie privée ou autrement répréhensible, y compris le contenu qui constitue de la pédopornographie, se rapporte à la bestialité ou dépeint des actes sexuels non consensuels.
- **Contenu nuisible :** Contenu malveillant et maliciel, tel que les virus, les chevaux de Troie, les vers, etc.
- **Contenu de spam :** Contenu publié à des fins de "black hat SEO", en utilisant des astuces telles que le link building / link spam, le keyword spam, afin d'exploiter la réputation des services Oxygis pour promouvoir du contenu, des biens ou des services de tiers.

Le Client reste seul responsable de la conformité des données hébergées ou traitées via les services Oxygis Cloud aux lois et réglementations applicables, notamment le Règlement Général sur la Protection des Données (RGPD).

II. Violations de la sécurité

Vous ne pouvez pas tenter de compromettre les services d'Oxygis Cloud, d'accéder ou de modifier du contenu qui ne vous appartient pas, ou de vous livrer à d'autres actions malveillantes :

- **Accès non autorisé :** accéder ou utiliser tout système ou service d'Oxygis Cloud sans autorisation.
- **Recherche en matière de sécurité :** effectuer toute recherche ou audit en matière de sécurité sur les systèmes Oxygis Cloud sans autorisation écrite à cet effet, y compris via des scanners et des outils automatisés. Veuillez consulter notre document de ***divulgation responsable*** pour plus d'informations sur la recherche en matière de sécurité d'Oxygis.
- **Écoute :** écouter ou enregistrer des données qui ne vous appartiennent pas sans autorisation.
- **Autres attaques :** attaques non techniques telles que l'ingénierie sociale, le phishing ou les attaques physiques contre toute personne ou tout système.

III. Abus de réseaux et de services

Vous ne devez pas abuser des ressources et des systèmes d'Oxygis Cloud. En particulier, les activités suivantes sont interdites :

- **Abus de réseau :** provoquer un déni de service (DoS) en inondant les systèmes de trafic réseau qui ralentit le système, le rend inaccessible ou a un impact significatif sur la qualité du service.
- **Appels RPC/API non étranglés** : envoi d'un grand nombre d'appels RPC ou d'appels API distants à nos systèmes sans étranglement approprié, avec le risque d'avoir un impact sur la qualité du service pour les autres utilisateurs. Remarque : Oxygis fournit des API par lots pour les importations, ce qui ne devrait pas être nécessaire. Les appels limités sont généralement acceptables pour une utilisation non soutenue, à raison d'un appel par seconde, sans appels parallèles. Des exceptions peuvent être autorisées au cas par cas pour Oxygis Cloud (veuillez **nous contacter** si vous pensez en avoir besoin), le mode d'hébergement dédié peut être considéré comme une alternative à cette restriction. Toute automatisation (y compris l'usage de bots, scripts ou intégrations externes) interagissant avec le Logiciel ou ses API doit rester raisonnable, documentée et conforme aux bonnes pratiques. Oxygis se réserve le droit de restreindre ou bloquer tout comportement automatisé perturbant la stabilité ou la sécurité de la plateforme.
- **Surcharge :** impact volontaire sur les performances ou la disponibilité des systèmes avec un contenu anormal tel que de très grandes quantités de données, ou un très grand nombre d'éléments à traiter, comme les bombes électroniques.

- **Crawling :** exploration automatique des ressources d'une manière qui a un impact sur la disponibilité et les performances des systèmes.
- **Attaquer :** utiliser les services Oxygis Cloud pour attaquer, crawler ou impacter de toute autre manière la disponibilité ou la sécurité de systèmes tiers.
- **Inscriptions abusives :** utilisation d'outils automatisés pour s'inscrire ou s'abonner de manière répétée aux services d'Oxygis.

IV. Conséquences en cas de violation

En cas de non-respect de la présente politique, Oxygis se réserve le droit de suspendre ou de restreindre l'accès du Client à ses Services. Lorsque cela est possible, une notification préalable sera envoyée pour permettre au Client de corriger la situation.
En cas de violation grave, intentionnelle ou répétée, Oxygis se réserve le droit de suspendre l'accès immédiatement, sans remboursement.