Vortex

Acceptable use policy

Last updated: November 2, 2026
https://www.vortexvip.org/en/acceptable-use

This page is a translation of the Spanish original. If they differ, the Spanish version prevails.

1. Purpose of the policy

The Vortex Acceptable Use Policy (AUP) sets the rules, limits and prohibitions that govern the proper use of our streaming/OTT platform by the Client. Its goal is to make sure the Service is used in a legal, ethical and respectful way, protecting both the integrity of the Vortex infrastructure and the rights of third parties. By accepting the Terms of Service and using Vortex, the Client also agrees to comply with this Acceptable Use Policy. Breaching this AUP may lead to corrective measures by Vortex, including suspension or termination of the service, as described below.

Since Vortex provides technology that can be used as a «bridge» and service platform to deliver content to end users, it is essential to define which uses are allowed and which are prohibited. This AUP applies both to the Client's direct actions on the platform and to the actions of the Client's end users when they access the streaming services supported by Vortex. The Client undertakes to inform its end users of these guidelines and enforce them, since it will be held responsible for the activities they carry out in the context of the platform.

2. Permitted use of the service

The Client and its end users must use Vortex only for legitimate purposes and in line with its intended purpose: distributing authorized audiovisual content to an audience entitled to access it, using the technical tools provided. The Service must be used following the recommended technical guidelines (for example, setting the streaming parameters properly) to ensure optimal performance. The Client will diligently keep its administration credentials confidential and watch its environment to prevent unauthorized access or abusive use.

In general, acceptable use is use that: (a) complies with all applicable laws (local, national and international); (b) respects the rights of third parties (copyright, trademarks, privacy, honor, etc.); (c) does not interfere with the normal operation of the platform or with the experience of other users or clients; and (d) does not involve fraudulent or malicious activities, or activities that may harm Vortex or anyone else.

Vortex may ask the Client, at any time, for its identification and the licenses for the content it offers. If the Client does not provide them within 10 business days, Vortex may disable the affected channel or titles.

3. Prohibited activities

It is strictly prohibited to use the Vortex Service (whether by the Client or by enabling its end users to do so) to carry out, promote or allow any of the following illegal or inappropriate activities:

- **Infringement of copyright or other intellectual property rights:** it is not allowed to upload, host, reproduce, retransmit, distribute or in any way disseminate through Vortex content for which the Client (or its users) does not hold the necessary rights. This includes, among others, transmitting

films, series, sports events, TV channels, music or other copyrighted material without the rights holder's authorization. Any form of piracy or unauthorized streaming is prohibited. In particular, it is prohibited to: resell or redistribute third-party channels or signals without a license; upload lists or links obtained from unauthorized services; offer «lifetime» access or «all channels» packages without licenses to back them; use brands of channels, leagues or studios without authorization; and use the platform to evade blocks ordered by an authority. The Client must make sure it holds valid licenses for any content it offers to its end users. Using the Service to infringe trademarks, patents, trade secrets or other intellectual property rights of third parties is also prohibited.

- **Use for illegal activities:** it is prohibited to use the platform as a means to commit or facilitate crimes, civil offenses or any breach of regulations. For example, Vortex may not be used to: distribute material that promotes terrorism or unlawful violence; plan or coordinate criminal activities; spread propaganda that could constitute a hate crime; or engage in fraud, computer scams or any criminal activity. Likewise, use in connection with unauthorized gambling, illegal betting or any activity that breaches local or international regulatory laws is forbidden.
- **Obscene, abusive or prohibited content:** the Client must not use Vortex to transmit content that is manifestly illegal, harmful or unacceptable. This includes, without limitation: child pornography or any material of sexual exploitation of minors (which will be reported to the authorities immediately if we detect it); content that incites extreme violence or hatred against protected groups; defamatory or slanderous material about third parties; extremely violent or cruel images or videos, or ones that glorify crimes. Although Vortex does not proactively monitor content (see the Privacy policy (https://www.vortexvip.org/en/privacy)), upon any valid notice of such prohibited content we may require the Client to remove it immediately.
- **Computer security, hacking and malware:** the Service must not be used to spread viruses, worms, trojans or other malware, or to launch computer attacks of any kind (for example, DDoS denial-of-service attacks, phishing, malicious port scanning, brute-force attacks on other systems, etc.). Using the Vortex infrastructure as a means of unauthorized intrusion into other systems, networks or accounts is likewise prohibited. Any attempt to breach the security of the Vortex platform or of other sites (including unauthorized pentesting, reverse engineering of the Vortex software beyond what is allowed, or exploiting vulnerabilities) will be a serious breach. Nor must the Client allow its end users to use the app or service for hacking or for activities that compromise cybersecurity.
- **Resource abuse and disruption of the service:** any use that interferes with the stability, integrity or availability of the platform is prohibited. Examples: actions that place a disproportionate load on the Vortex servers (for example, high-frequency automated scripts that flood the APIs without authorization, or multiple simultaneous connections outside the normal contracted streaming parameters); trying to saturate the bandwidth or capacity of the system beyond the agreed limits; or tampering with the app to gain undue advantages (such as evading user concurrency controls, or modifying the app client to access features that are not allowed). Unauthorized «restreaming» is also prohibited, meaning the retransmission or redistribution of streaming signals obtained through Vortex to third parties or outside the original target audience, without consent. For example, an end user of the Client must not capture a signal received through the Vortex app and republish it on another platform; the Client must take contractual and technical measures to prevent this, and Vortex may suspend the service if it detects that the Client itself is massively redistributing content to third parties not covered by the contract.
- **Spam, phishing and deceptive activities:** the Client will not use the Vortex communication

channels (for example, push notifications or emails sent from the platform) to send unsolicited bulk messages (spam) with unauthorized advertising, or to run phishing or impersonation campaigns. The Client will only send emails to end customers who have authorized it or with whom it has a current contractual relationship, and every commercial email will allow unsubscribing. Nor will usernames, identifiers or any integration with the platform that seeks to pass as another person, company or entity deceptively with intent to defraud be allowed. In general, any deceptive or fraudulent conduct towards end users or third parties through Vortex is prohibited (for example, creating a «mirror» service that imitates another brand to confuse users).

- **Kids' profiles:** it is prohibited to use kids' profiles to show unsuitable content or advertising, or to collect more data than necessary.
- **Other abusive conduct:** any other activity not listed above that is clearly contrary to the spirit of legitimate use of the Service, or that may be considered abusive, harmful or unlawful, is also prohibited. This includes privacy violations (for example, using the platform to collect end users' personal data unlawfully), publishing content that violates privacy or confidentiality rights, hosting non-consensual pornography or «revenge porn», etc. It is also expressly prohibited to try to evade, remove, disable or circumvent the technical protection or monitoring measures that Vortex has implemented in the Service (for example, anti-piracy systems, DRM, connection limits, etc.), or to help or instruct others to do so.

The list above is illustrative and not exhaustive. If there is reasonable doubt about whether an activity is allowed, the Client must consult Vortex first or assume the most restrictive interpretation.

4. No active monitoring

Vortex does not actively or generally monitor the content that Clients or their end users transmit through the platform, nor the specific activities they carry out, except to the extent needed for technical operation (for example, performance monitoring) or where we are legally required to do so in specific cases. In other words, by default Vortex does not exercise censorship or editorial supervision over the Client's content, nor does it examine each transmission looking for infringements. This approach is based on international legal frameworks that do not impose on service providers a general obligation to monitor the information they store or transmit, or to actively seek facts indicating illegal activity.

Vortex does not review all content, but it acts when it receives a valid notice or when evident facts show an infringement.

However, Vortex reserves the right to investigate internally any possible breach of this Acceptable Use Policy when there are elements or indications that warrant it (for example, after receiving third-party notices of alleged abuse, system alerts about anomalous activity, or an order from a competent authority). Such an investigation may involve a limited review of the Client's information related to the suspicion (for example, examining the relevant logs, checking settings or, in extreme cases, temporarily accessing fragments of content to verify whether it breaches the rules, always keeping confidentiality). This kind of access will be done with the utmost care and only to verify compliance with the AUP or the law.

We reiterate that, in general, Vortex only reacts to illegal content or uses when it has actual knowledge of them, usually through formal complaints, notices from authorities or from recognized rights holders. In that case, as described in the Copyright and takedown policy (https://www.vortexvip.org/en/copyright), we will notify the Client and take the appropriate measures. As long as there is no such knowledge,

Vortex acts in good faith assuming that the Client operates within the law and this Policy.

5. The Client's responsibility for its end users

The Client must make sure that its end users (subscribers, customers or any third party to whom it gives access to content through Vortex) also comply with the guidelines of this Acceptable Use Policy. It is the Client's responsibility to inform its users about the terms of use of its streaming service, including which behaviors are prohibited. For example, the Client should include in its own terms with its subscribers clauses that forbid them from: sharing their credentials with unauthorized people, trying to download or restream the content without authorization, using the service for unlawful purposes, etc., in line with this AUP.

If an end user of the Client engages in any of the prohibited activities above (for example, if a subscriber is redistributing a channel to third parties without permission, or uploading illegal content to a user-generated content feature of the platform, if one existed), the Client must act promptly to stop that activity and, if necessary, suspend or cancel that user's access to its service. Vortex will cooperate with the Client by providing reasonable information (for example, logs) that may help identify internal abuse, always in compliance with privacy law.

Ultimately, the Client assumes responsibility for the acts of its end users on the platform. Vortex will consider the Client responsible for any indirect breach committed by its users, since it is the one that gave them access to the system. This means that, if an end user breaks the rules, Vortex may have to step in and even suspend the Client entirely (if the Client does not act or the problem recurs), although ideally it will be solved by isolating the offending user. It is therefore in the Client's interest to watch over the proper use by its end users and to have ways to detect improper behavior (for example, multiple suspicious logins, unusual consumption patterns, etc.).

Resellers: the Client answers for its resellers. Each reseller must accept this Policy before using the portal. Vortex may disable a reseller that breaches it and will notify the Client.

6. Consequences of misuse

A breach of this Acceptable Use Policy by the Client (or its end users) is considered a material breach of the terms of service and entitles Vortex to take the measures it deems necessary to remedy the situation and protect its interests and those of third parties. Depending on the seriousness of the case, these measures may include:

- **Warning and request to remedy:** for less serious or remediable breaches (for example, the inadvertent use of unlicensed content), Vortex may notify the Client describing the breach detected and requesting corrective action within a set period. The Client must respond and take immediate measures to stop the breach, or provide clarifications or documentation that justify the activity.
- **Temporary suspension of the Service:** if the breach is serious or repeated, or poses an imminent risk to the platform or to third parties, Vortex will suspend the Service partially or fully with immediate effect, without prior notice in critical cases. Suspension may involve blocking the Client's access to the backend, temporarily disabling the delivery of streams or isolating the account. This measure aims to prevent greater harm while the matter is investigated or until the Client guarantees that the abuse has stopped. Vortex will inform the Client of the suspension and its reasons as soon as possible. During a suspension, the Client remains obliged to pay the applicable fees and will not be entitled to a refund for the suspended period, since the cause is a breach of the AUP.

- **Termination of the service (account cancellation):** in cases of serious or illegal breaches, or if the Client ignores our warnings and continues or repeats prohibited uses, Vortex may terminate the contract and permanently close the Client's account, as provided in the Terms of Service. This termination for cause will mean loss of access to the platform, deletion of the Client's data and Vortex's possible refusal to enter into future business relationships with that Client. No refund for unused services will be due in this case either, since the termination is attributable to the Client. Vortex will notify the Client of the termination decision, stating the reasons.
- **Further legal action:** if the Client's misuse causes damage to Vortex (for example, harm to the infrastructure, legal penalties or third-party claims against Vortex) or breaches criminal or civil law, Vortex reserves the right to take the relevant legal action to seek redress. This may include cooperating with the authorities by filing complaints (for example, if distribution of child pornography is detected, Vortex will report it immediately to the competent authorities and provide the necessary information), or bringing civil claims against the Client for compensation for the damage caused by the prohibited conduct.

In addition, Vortex may block or remove any content hosted on the platform that is proven to breach this AUP, without any liability. For example, if after due process it is confirmed that a certain channel or video infringes copyright and there is no legal basis to keep it, we could remove it from the system. As far as possible, it will be preferred that the Client itself removes the disputed content; Vortex will step in directly only if the Client does not cooperate or in urgent situations.

Vortex keeps a record of every warning, suspension and termination, with the date and the reason.

The Client understands that Vortex is not obliged to monitor or guarantee the behavior of end users, but has the power to enforce these rules for the common good of the platform and its community of clients. No omission or delay by Vortex in exercising a right under this AUP shall be interpreted as a waiver of that right in the future.

7. Vortex's right to update this AUP

The internet and the forms of abuse evolve constantly. Vortex reserves the right to modify this Acceptable Use Policy as needed to address new risks or to adapt to legal changes. If it is updated, we will notify the Client (for example, by email or with a message in the console), indicating the new version of the AUP or the material changes. It is the Client's responsibility to review those notices. Continued use of Vortex after the update takes effect will constitute acceptance of the amended AUP. If the Client does not agree with the changes, it may terminate the service before they take effect, following the cancellation procedure provided.

In short, we want to foster a safe and legitimate environment for all our clients. We appreciate the Client's cooperation in following these guidelines and invite it to report any misuse or security vulnerability it detects. Together we can make sure Vortex remains synonymous with trust and quality in OTT content distribution.

Note

Vortex reminds you that it does not proactively monitor the Client's content except where legally required, and that it does not offer technical support or direct advice to the Client's end users; compliance with the rules by end users must be managed by the Client itself within its own sphere.

Contact: soportevortextv@gmail.com · WhatsApp +506 8346 1166