

Acceptable Use Policy

What may and may not run on our infrastructure.

Key points for reference

- Lawful use that respects people and their data.
- No fraud, unauthorized access, malware or spam.
- Proportionate containment and review.

Reference summary. The complete clauses below prevail.

1. People and activities covered

The AUP covers customers, representatives and users of websites, applications, email, integrations, bots and public tools under their administration. Customers communicate relevant rules and address known misuse without automatic liability for every third-party act.

Using a resource does not authorize access to others' accounts, data, networks or devices. Orders and licenses govern resources. Lawful criticism, complaints and exercising rights are not abuse by themselves.

2. Unlawful activity and rights infringement

Fraud, phishing, credential theft, deceptive impersonation, child exploitation, trafficking, nonconsensual intimate disclosure, criminal incitement to violence and unlawful discrimination are prohibited. So are unlawful commerce and distribution lacking required authority or legal basis.

Assessment considers law, evidence, context and Zovvi's role. Disagreement does not make an opinion unlawful. Notices identify resources and facts; reporting does not automatically mean removal.

3. Network security and integrity

Malware, ransomware, botnet control, unauthorized exploitation, traffic interception, brute force, credential distribution and denial of service are prohibited. Do not host malicious files to attack Zovvi or others.

Responsible research is not blanket permission: risky scanning or exploitation beyond normal account use requires written scope. Public noninvasive tools have their own limits. Stop exploration on encountering others' data and report minimal evidence.

4. Messages, data and privacy

Do not send spam, conceal senders, use purchased or abusively collected lists, bypass opt-outs or exploit compromised mailboxes. Messages need lawful purposes and email-policy compliance; SPF or unused quota does not authorize abuse.

Third-party data and materials require authority. Publishing credentials, leaked databases or unlawfully obtained data is prohibited. Hosting does not automatically take over customer visitor-data purposes; roles depend on activity and law.

5. Resources, automation and shared environments

Keep CPU, memory, I/O, processes, storage and sending within the plan. Do not evade isolation, quotas or authentication through multiple accounts or distributed automation. Website hosting is not unrestricted repositories, mining or unpurchased intensive processing.

Bots and tasks need consumption controls. Legitimate peaks require diagnosis rather than automatic violation findings. Objective limits must be disclosed in advance; fair use does not create hidden post-purchase limits.

6. Incident handling and measures

Evidence and impact are assessed. Measures may include correction guidance, sending or process limits, isolation and necessary suspension. Measures must be proportionate, limiting the affected component where protective. Urgent risks or valid orders may require action before notice.

Reasons, scope and resolution conditions are recorded without unnecessarily exposing reporters or safeguards. Severity or recurrence may justify lawful termination. Containment does not authorize exploiting or disclosing customer data.

7. Reports, challenges and rights

Use Report abuse for suspicious resources and Report a bug for platform defects. Provide URLs, facts, dates and minimal evidence without illegal files, passwords or others' databases. Intellectual-property notices follow that policy. Do not intimidate reporters or seek removal of lawful content.

Affected customers may request review and provide context. Authority preservation or disclosure requires a valid basis and standing. The AUP does not remove rights or permit abusive withholding of funds or data.