

Política de Uso Aceitável

O que pode e o que não pode passar pela nossa infraestrutura.

O essencial para consulta

- Uso lícito, com respeito às pessoas e aos seus dados.
- Nada de fraude, invasão, malware ou spam.
- Contenção proporcional e possibilidade de revisão.

Resumo de consulta. As cláusulas completas abaixo prevalecem.

1. Quem e quais usos estão abrangidos

A AUP se aplica ao cliente, representantes e usuários que utilizam os recursos sob sua administração, inclusive sites, aplicações, e-mails, integrações, bots e ferramentas públicas. O cliente deve informar regras pertinentes à sua equipe e agir quando souber de uso indevido, sem presumir responsabilidade automática por todo ato de terceiro.

A permissão de usar um recurso não autoriza acesso a contas, dados, redes ou dispositivos de outra pessoa. Recursos e licenças seguem o pedido. A liberdade de crítica, reclamação ou exercício de direitos não é considerada abuso por si só.

2. Atividades ilegais e violação de direitos

É proibido usar a infraestrutura para fraude, phishing, roubo de credenciais, falsificação enganosa de identidade, exploração de crianças, tráfico de pessoas, divulgação íntima sem consentimento, incitação criminosa à violência ou discriminação ilícita. Também são proibidos comércio ilegal e distribuição de conteúdo sem autorização ou fundamento legal quando exigidos.

A análise considera a lei aplicável, a evidência, o contexto e o papel da Zovvi. Não basta discordar de uma opinião para torná-la ilícita. Notificações devem identificar o recurso e os fatos; medidas legais urgentes seguem o regime pertinente, sem prometer que toda denúncia gera retirada automática.

3. Segurança e integridade da rede

São proibidos malware, ransomware, comando e controle de botnets, exploração de vulnerabilidades sem autorização, captura indevida de tráfego, força bruta, distribuição de credenciais e negação de serviço. Não hospede arquivos maliciosos para distribuição nem use o plano para atacar a própria Zovvi ou terceiros.

Pesquisa responsável não é autorização geral de teste: qualquer atividade além do uso comum da

própria conta deve ter escopo escrito quando envolver risco, varredura ou exploração. Consultas públicas não invasivas oferecidas pelas ferramentas têm limites próprios. Ao encontrar dados alheios, interrompa a exploração e relate somente a evidência mínima.

4. Mensagens, dados e privacidade

Não envie spam, oculte a identidade do remetente, use listas compradas ou coletadas abusivamente, contorne descadastrados ou explore caixa comprometida. Mensagens legítimas precisam de finalidade lícita e cumprimento das regras específicas de e-mail. Ter SPF ou um limite de envio disponível não autoriza campanha abusiva.

Dados pessoais e materiais de terceiros exigem legitimidade para tratamento e uso. É vedado publicar credenciais, bases vazadas ou dados obtidos ilegalmente. A hospedagem não decide, por padrão, as finalidades do banco de visitantes do cliente; a divisão de papéis e obrigações decorre da atividade e da lei.

5. Recursos, automação e ambiente compartilhado

Utilize CPU, memória, I/O, processos, armazenamento e envios dentro do plano. Não contorne isolamento, cotas, autenticação ou limites, inclusive com contas múltiplas ou automações distribuídas. Hospedagem de site não equivale a repositório público irrestrito, armazenamento de terceiros, mineração ou processamento intensivo não incluído.

Bots, tarefas e integrações devem ter controle de frequência, credenciais e consumo. Picos legítimos exigem diagnóstico e dimensionamento, não presunção automática de infração. Limites objetivos devem ser informados previamente; “uso justo” não autoriza inventar um limite oculto depois da contratação.

6. Tratamento de incidentes e medidas

Ao identificar risco, avaliamos evidência e impacto. Podemos orientar correção, limitar envio ou processo, isolar arquivo ou recurso e, quando necessário, suspender o serviço. A medida deve ser proporcional, preferindo conter o componente afetado se isso proteger os demais usuários. Risco urgente ou ordem válida pode exigir ação antes do aviso, com comunicação posterior assim que permitida.

A Zovvi registra fundamento, alcance e condições para regularizar, sem expor desnecessariamente dados de denunciante ou técnicas de proteção. Reincidência ou gravidade pode justificar rescisão conforme contrato e lei. A contenção não é autorização para explorar ou divulgar dados do cliente.

7. Relato, contestação e direitos

Use Denunciar abuso para recurso suspeito e Reportar bug para defeito da plataforma. Informe URL, fatos, datas e evidência mínima; não envie arquivos ilegais, senhas ou bases de terceiros. Notificações de propriedade intelectual seguem a política específica. Não use o canal para ameaçar ou pressionar retirada de conteúdo lícito.

O cliente afetado pode pedir revisão e apresentar contexto pelo atendimento. Obrigações de preservação e fornecimento a autoridades dependem de fundamento e legitimidade, não de qualquer solicitação informal. Esta AUP não afasta direitos legais ou permite retenção abusiva de valores e dados.

