

Anti-Spam Policy

Send messages people expect to receive.

Key points for reference

- Legitimate sending needs justified sources and purposes.
- Buying a list does not prove permission.
- We protect delivery without promising perfect filtering.

Reference summary. The complete clauses below prevail.

1. Scope and prohibited messages

This covers email, forms, accounts and automation on Zovvi resources. Spam, phishing, malware, fraud, forged origins and abusive forwarding are prohibited. Volume alone does not define spam; individual messages may be abusive. Compromised accounts require containment and correction even without owner intent.

2. Recipient sources and identity

Senders must demonstrate legitimate sources, compatible purposes and legal grounds. Consent must be specific and verifiable where used. Purchased, scraped or unknown-origin lists do not prove marketing permission.

Accurately identify sender, domain and subject. Do not disguise advertising as urgent security or billing. Transactional messages must reflect real relationships rather than serve as campaign pretexts.

3. Unsubscription and hygiene

Marketing needs a simple working opt-out without requiring a password. Applicable objections or withdrawal must be honored before further sending. Suppression lists may retain only what prevents re-enrollment.

Remove invalid addresses and handle bounces and complaints. Do not repeatedly retry blocked or unsubscribed recipients. Lack of complaints does not prove lawful sourcing.

4. Authentication and limits

Configure SPF, DKIM and DMARC and protect credentials and forms. Standard hosting is not a bulk-mail platform. Limits depend on the disclosed plan; multiple accounts must not evade queues.

Filters, reputation and recipient policies affect delivery. Inbox placement and complete spam elimination are not guaranteed. Allowlisting must not improperly disable malware or spoofing protections.

5. Investigation and remediation

Evidence may justify proportionate sending limits, queues or isolation. Review considers headers, necessary logs, sources, complaints and compromise with confidentiality and minimization. Whole operations should not be suspended where a narrower measure suffices.

Customers receive cause, remediation and review guidance where possible. Reactivation may require credentials, application fixes, source evidence and volume adjustments. Fraud or serious recurrence may lead to lawful termination.

6. Reporting

Use Report Abuse or ola@zovvi.com.br with date, sender, recipient and relevant headers, removing secrets and excess data. Do not forward malicious attachments. Receipt does not prove a violation. Affected users may supply context and request review without losing legal rights.