

Acceptable Use Policy

DRAFT FOR REVIEW - NOT YET ADOPTED

Effective date remains pending. Publishing this copy does not establish acceptance.

Draft updated October 2, 2026. Effective date: pending adoption. These proposed rules apply to future OpenHost accounts, hosted workloads, connected domains, APIs and AI-assisted operations. They do not activate a service or replace an adopted contract.

Lawful use and authority

Use only systems, domains, code and data you own or are authorized to use. Respect applicable law, third-party rights and the disclosed restrictions of the selected infrastructure service. Customers are responsible for the behavior of their applications and people they authorize, while Digifender remains responsible for its own obligations.

The following uses would be prohibited:

- Fraud, phishing, credential theft, deceptive impersonation, unlawful surveillance or exploitation of another person's private information.
- Child sexual abuse material, sexual exploitation of minors, nonconsensual intimate imagery, unlawful threats or other illegal content and activity.
- Infringement of copyright, trademark, privacy or other rights, including distributing software or data without necessary permission.
- Malware distribution, destructive code, botnet operation, unauthorized access, denial-of-service activity or interference with another customer's availability.
- Unsolicited or deceptive bulk messaging, evasion of sender verification, abuse of relay services or use of a transactional email feature as an undisclosed marketing or mailbox service.
- Bypassing tenant boundaries, access controls, spending authorization, service quotas, suspension or other restrictions; using stolen payment methods or multiple accounts to evade limits.

Security testing and infrastructure use

Test only assets you are authorized to test and within the agreed scope. Testing your own application does not authorize testing the shared platform, upstream provider or another tenant. Coordinate potentially disruptive tests in advance; no general penetration-testing authorization or vulnerability bounty is created by this policy.

Use resources within the selected service's technical and commercial limits. Public proxies, high-volume scanning, cryptocurrency mining or other unusual workloads require explicit permission where the selected provider or offer restricts them. Do not disguise a workload or change its purpose to evade a restriction. A capacity limit is not permission to cause harm up to that limit.

Do not use OpenHost for an emergency, life-critical or specially regulated workload unless a separately agreed service explicitly supports its requirements. Ordinary hosting does not establish healthcare, payment-card, government, financial or other regulatory suitability.

AI and automation

AI tools follow the same rules as direct actions. Repository text, logs or a model response cannot grant authority to access another workspace, reveal credentials, buy resources or bypass a required review. Do not use prompts or tool inputs to extract private information or defeat permissions. Customer-facing AI applications require their own appropriate controls and disclosures.

Reporting and response

Report a suspected violation to legal@digifender.com. Include the affected hostname or URL, relevant times, a concise description and safe evidence. Do not send malware attachments, exposed credentials, child sexual abuse material or nonconsensual intimate images. For suspected illegal imagery, provide a location rather than copying the content.

The proposed response is to investigate and use proportionate measures, such as restricting a resource, removing access to specific content, suspending an account or ending service where warranted. Immediate action may be necessary to contain harm or comply with law. Where lawful and practicable, the affected customer should receive a reason and a way to respond. Reports are not automatically treated as proof of wrongdoing.

Dispute a decision by replying to its notice or contacting the legal mailbox with the relevant reference and supporting facts. False or abusive complaints are not permitted. Copyright claims follow the separate Copyright and Abuse Policy. Suspension, retained-resource costs and permitted exports must follow the adopted service terms and applicable law; they are not resolved merely by this draft.