Acceptable Use Policy

AUP / Abuse Rules

Stand: 2026-05-02

Rules against spam, attacks, illegal content and harmful use of OpenDucks IT services.

1. Scope

This Acceptable Use Policy applies to all OpenDucks IT services, including hosting, cloud, mail, VPN, managed services, support, software and infrastructure.

2. Prohibited Use

Customers must not use services for illegal, harmful, deceptive, abusive or disruptive activity. This includes phishing, scams, credential theft, malware, botnets, ransomware, spam, unsolicited bulk messaging, DDoS, unauthorised scanning, exploitation attempts, copyright infringement, fraud and harassment.

Customers must not attempt to bypass security controls, rate limits, account restrictions, billing systems or service boundaries.

3. Mail and Messaging

Mail services must not be used for spam, mail bombing, forged headers, list abuse, phishing, malware distribution or unsolicited bulk messaging.

Customers are responsible for securing forms, websites and applications that can send email.

4. Security Requirements

Customers must keep self-managed applications patched, protect credentials, use reasonable authentication measures and report suspected compromise promptly.

Open relays, exposed admin panels, vulnerable scripts or abusive traffic may lead to temporary restrictions.

5. Enforcement

OpenDucks IT may investigate abuse reports and take proportionate action, including notification, rate limiting, filtering, suspension, deletion of unlawful content, service termination or escalation to authorities.

Severe abuse may require immediate action without prior notice.

Kontakt

Fragen zu diesem Dokument können an legal@openducks.org gerichtet werden. Abuse-Meldungen bitte an abuse@openducks.org oder über die Abuse-Seite einreichen.