ZOP IT

Security & Trust Whitepaper

How Zop It protects customer content and data.

Zop It is built for organizations that host confidential and proprietary material. Security and tenant isolation are designed into the platform from the ground up — not added as an afterthought. This document summarizes the safeguards we have in place to protect your assets.

Prepared for:	Prospective customers and security reviewers
Last updated:	June 2026
Document version:	1.0
Security contact:	security@zopit.space

Security at a glance

Zop It is a B2B platform built for organizations that host confidential and proprietary material. The following pillars summarize how we protect your assets; each is detailed in the sections that follow.

Tenant Isolation

Every organization's content and data are segregated at the database level and enforced on every request, so no customer can ever reach another customer's assets.

Encryption

Data is encrypted in transit with TLS (HTTPS enforced) and encrypted at rest by our infrastructure providers using industry-standard AES-256.

Access Control

Role-based permissions, per-account scoping, and short-lived signed links for confidential media ensure people only ever see what they are authorized to.

Secure Infrastructure

We build on Vercel and Supabase — both independently audited to SOC 2 Type II — inheriting enterprise-grade physical, network, and platform controls.

Continuous Testing

We run regular internal penetration tests and security reviews, simulating real attacks against the live platform and remediating findings on a documented schedule.

Secure Authentication

Managed authentication with hashed credentials, scoped sessions, and privilege-escalation protections that prevent users from elevating their own access.

Data isolation & multi-tenancy

Zop It is a multi-tenant platform, but your data is never co-mingled with another organization's in a way that anyone can access.

- Row-Level Security (RLS) is enforced in the database, so isolation is guaranteed by the data layer itself — not just by application code.
- Every request that touches customer data is scoped to the authenticated account on the server before any data is returned.
- We validate isolation with live intrusion testing that attempts cross-tenant access using only the credentials an outside attacker could obtain.

Encryption & data protection

- All traffic is served exclusively over HTTPS/TLS, with HTTP Strict Transport Security (HSTS) enforced in

production.

- Data at rest is encrypted by our database and file-storage providers using AES-256.
- Confidential media is delivered through short-lived, signed URLs that expire automatically and cannot be guessed or shared indefinitely.
- Modern security response headers (content-type protection, referrer policy, framing/clickjacking protection on sensitive pages) are applied across the platform.

Access control & authentication

- Role-based access separates platform administrators, channel owners, and viewers, with each role limited to its own scope.
- Authentication is handled by a managed identity provider; passwords are salted and hashed, never stored in plain text.
- Session and one-time-code data is locked to privileged backend access only and is never exposed to the browser.
- Sensitive account attributes (such as roles and subscription level) cannot be modified by end users — only by trusted server-side processes.

Payments & financial data

- All payment processing is handled by Stripe, a PCI-DSS Level 1 certified provider.
- We never see, handle, or store raw card numbers — sensitive cardholder data stays within Stripe's certified environment.
- Payout and billing configuration is restricted to authorized account owners and trusted backend processes.

Application security & testing

- We perform regular security audits covering database access rules, API endpoints, file uploads, and dependencies.
- Uploaded files are served with protections that neutralize active-content attacks (for example, scripts embedded in image files).
- Third-party dependencies are monitored for known vulnerabilities and patched promptly.
- Abuse and cost-control limits protect platform availability against automated misuse.

Platform integrity & brand protection

We actively protect the integrity of the platform so your brand is never associated with impersonators or bad actors operating alongside you.

- New channels are screened against a maintained blocklist of well-known brands, organizations, and platforms to prevent impersonation at signup.
- Our matching normalizes common evasion tricks — look-alike spellings, leetspeak, and symbol substitutions — so impersonation attempts cannot slip through with minor tweaks.
- Brand-name enforcement runs server-side and cannot be bypassed by client-side manipulation; it applies to channel creation, renames, and account signup alike.
- Attempts to register a protected brand are blocked and routed to our team for review, keeping the marketplace trustworthy for legitimate publishers.

Hosting & sub-processors

We rely on a small set of established, independently audited providers. We are happy to share our full sub-processor list during a security review.

- Vercel — application hosting and content delivery (SOC 2 Type II).
- Supabase — database and authentication (SOC 2 Type II).
- Vercel Blob — encrypted file and media storage.
- Stripe — payment processing (PCI-DSS Level 1).

Compliance & data governance

Zop It is operated by Orione OÜ, a company registered in Estonia (registration number 14749724), and hosts data on infrastructure located within audited, reputable cloud regions.

Our platform is built on SOC 2 Type II-certified infrastructure, and we follow aligned operational practices internally. For enterprise engagements we can support:

- Data Processing Agreements (DPA) for GDPR-aligned engagements.
- Completed security questionnaires (such as CAIQ-Lite or SIG-Lite) on request.
- Documented data export and deletion procedures for your organization's data.
- Discussion of additional controls — such as single sign-on (SSO) and audit logging — as part of an Enterprise plan.

Some certifications and capabilities are available on specific plans or on our roadmap. We are glad to walk through current status and timelines during a security review.

Responsible disclosure

We take security reports seriously. If you believe you have found a vulnerability, please contact our security team directly so we can investigate and respond quickly. We appreciate responsible disclosure and will work with you to resolve verified issues.

Security contact: security@zopit.space

Talk to our team

We are happy to support your security review — including questionnaires, a Data Processing Agreement, and a walkthrough of our controls.

- Sales & security reviews: sales@zopit.space
- Website: https://zopit.space