Screenzor

Vulnerability Disclosure Policy

Last revised: July 24, 2026

We take the security of screenzor.com, the Screenzor Chrome extension, and our backend services seriously, and welcome reports from security researchers who find vulnerabilities in good faith.

1. Scope

This policy covers:

• screenzor.com and its subdomains;

• the Screenzor Chrome extension; and

• Screenzor's backend APIs.

It does not cover our infrastructure providers' own systems (e.g. Supabase, our cloud hosting provider, Google Analytics/Ads, Payfast, or Paystack) — please report issues in those systems directly to the relevant provider.

2. Reporting a Vulnerability

Email legal@screenzor.com with a description of the issue, the steps to reproduce it, and its potential impact. We aim to acknowledge reports within 5 business days and to keep you updated as we investigate and address the issue.

Please do not publicly disclose a vulnerability until we have had a reasonable opportunity to address it.

3. Safe Harbor

If you make a good-faith effort to comply with this policy during your security research, we will not pursue legal action against you for that research, including under the US Computer Fraud and Abuse Act (CFAA) or similar anti-hacking laws elsewhere, consistent with the approach described in the US Department of Justice's "Framework for a Vulnerability Disclosure Program for Online Systems." This safe harbor applies only to research that:

• stays within the scope described in Section 1;

• avoids privacy violations, destruction of data, and interruption or

degradation of the Service (no denial-of-service testing);

• does not access, modify, or exfiltrate other users' data — use only

test accounts you control; and

• gives us a reasonable opportunity to fix the issue before any public

disclosure.

4. Out of Scope

The following are not eligible for safe harbor or a response under this policy: social engineering or phishing of our users or any Screenzor personnel, physical attacks against our (or our providers') facilities, denial-of-service testing, and automated scanning that generates significant traffic without prior coordination with us.

5. Changes to This Policy

See the notice at the end of this document for how we handle changes to this policy.

Last revised: July 24, 2026

We may update this document from time to time. If we make material changes, we will notify you by email and/or a notice on the Screenzor website before the change takes effect. Minor changes will only update the date above.