

RESPONSIBLE DISCLOSURE & VULNERABILITY POLICY

Find a vulnerability? **Report it safely.** We won't come after you.

Version history: v1.0 — 25 October 2026 (initial publication). v1.1 — 25 October 2026 (audit fixes).
See </legal/CHANGELOG.md>

Digitaliisla Technologies Private Limited welcomes good-faith security research on the DigiSurvey platform. This policy sets out what is in scope, what is out of scope, how to report, how we will respond, and the **safe-harbour commitment** we make to researchers who follow this policy. It is one of the simplest promises we make: play fair with us, and we play fair with you.

1. Scope

- **In scope.** All subdomains of `*.digitaliisla.co.in` — the website, the DigiSurvey web application, the public and partner APIs, and the mobile applications (Android and iOS) once published.
- **Documented APIs** accessed with your own credentials, within the quota of your own account.
- **Our open-source repositories**, if any, as published from our GitHub organisation.

2. Out of scope

The following are not covered by this policy. Finding issues in these areas does not qualify for safe harbour under this policy and may lead to legal consequences; please do not attempt them on our behalf.

- **Physical attacks** on our offices, personnel, or facilities.
- **Social engineering** of our employees, contractors, directors, grievance officer, auditors, or vendors.
- **Denial-of-service (DoS / DDoS)** testing, resource-exhaustion tests, mass automated scanning that creates volume-based load, SMS or email flooding of our systems or our users.
- **Third-party services** we use — **Supabase, Cloudflare, Cloudflare R2, AWS S3 Mumbai, Backblaze, Razorpay, Resend, Zoho, Google Gemini** — are to be reported to those vendors directly under their own disclosure policies, not to us. We cross-reference them in our Sub-processors page.
- Attacks that **require physical access** to a user's unlocked device.

- Reports from **automated scanners** with no proof of exploitability (e.g. “TLS version supported” without a concrete attack).
- Issues that only affect **outdated browsers or clients** that we have explicitly deprecated.
- **Spam and phishing of other users** through platform features — this is also prohibited by the Acceptable Use Policy.

3. Safe harbour

Our commitment to researchers. If you make a good-faith effort to comply with this policy during your research, we will:

- Consider your research **authorised** under Section 43 of the Information Technology Act, 2000 and under our Terms of Service.
- **Not pursue civil or criminal legal action** against you, nor send a legal notice to your employer, your university, your hosting provider, or your government.
- Work with you to understand and remediate the issue quickly.
- **Credit you** publicly, with your permission, in our Hall of Fame (planned).

Safe harbour does not apply where the researcher knowingly exfiltrates or publishes real user data, extorts the Company, or attacks third parties through our systems. We reserve rights for conduct outside good-faith research.

Good-faith conditions

To stay inside safe harbour you must:

- Give us a **reasonable time to fix** before any public disclosure — see our fix timelines in Clause 5 and the 90-day coordinated-disclosure rule in Clause 7.
- **Not exfiltrate data** beyond the minimum needed to demonstrate the vulnerability — and when you do touch real user data accidentally, you stop, delete it, and tell us.
- **Not disrupt our service** or that of our users (so, no destructive proofs-of-concept, no mass automation, no DoS).
- Only interact with accounts you own or have explicit permission to test.
- Not use the finding to extort payment, access, or any other benefit.

4. How to report

- Email security@digitaliisla.co.in with:
 - A clear description of the vulnerability

- A **proof-of-concept** (steps, HTTP requests, a short screencast, or a script we can run locally)
- The **potential impact** (what an attacker could do, who could be affected)
- Any suggested fix, if you have one — appreciated, not required
- How you would like to be credited in the Hall of Fame (or that you'd prefer anonymity)
- **PGP key.** **Planned Q1 2027** — we will publish a PGP public key for encrypted reporting. Until then, email is fine; if your finding is extraordinarily sensitive, we can arrange a Signal or a secure channel on request.
- **Report to one place.** Please do not file the same issue in multiple inboxes (ticketing, support, social media). security@ is the right address and reaches on-call directly.

5. Our response SLAs

Milestone	Our commitment
Acknowledgement of your report	Within 24 hours of receipt — a real person, with a tracking reference.
Triage completed	Within 3 business days — severity assigned, scope confirmed, you're told whether safe harbour applies.
Fix — Critical (RCE, full tenant takeover, mass PII exposure)	7 days from triage; interim mitigation same-day if the fix cannot be shipped in hours.
Fix — High (authentication bypass, cross-tenant leak, injection with real impact)	14 days from triage.
Fix — Medium (information disclosure, business-logic abuse, missing security control)	30 days from triage.
Fix — Low (hardening, defence-in-depth, best-practice gap)	90 days from triage, or scheduled into the next quarterly hardening cycle.
Status updates	At least every 7 days until the issue is resolved, more often for critical and high.

6. Recognition

- **Hall of Fame.** **Planned Q1 2027** — we will publish a Hall of Fame on digitaliisla.co.in/security/hall-of-fame listing researchers (with their consent) and the general class of their finding. Until then we credit personally in our release notes and in writing to the researcher.
- **Monetary bounty.** **Under consideration for 2027** — we are evaluating a cash bounty programme once the volume of reports justifies it. In the meantime, exceptional reports may receive a goodwill token at the Directors' discretion. No researcher's eligibility for safe harbour depends on this.
- **Letter of thanks.** On request, we will send a formal, Director-signed letter of thanks on company letterhead — useful for CVs, university programmes, and bug-bounty platforms.

7. Public disclosure

- You may publish your write-up **once the fix has shipped, or 90 days after triage, whichever is earlier**. We follow the same clock.
- For a vulnerability where releasing details before patching would create meaningful ongoing risk to users, we will ask for an extension in writing with a dated reason; the researcher is free to refuse but we'd appreciate consideration.
- We will give you a copy of our own public post-mortem before publication, so you can confirm the attribution.

8. Alignment with Indian regulation

CERT-In Directions, 28 April 2022. For any vulnerability we must report under the CERT-In Directions (actively exploited vulnerabilities and specified classes of cyber incidents), **we file with CERT-In within 6 hours of confirmation**, as required by law. This is parallel to our researcher communication and does not reveal the researcher's identity without consent.

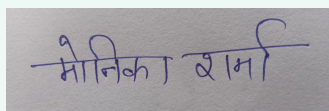
- **DPDPA 2023.** Where a confirmed vulnerability led to a Data Breach as defined under DPDPA 2023, we also follow our Breach Notification SOP — DPB notification within 72 hours, affected Data Principal notification promptly thereafter.
- **IRDAI.** Where the vulnerability is relevant to the Company's obligations in supporting IRDAI-licensed surveyors, the Company's designated regulatory contact handles the communication.
- **IT Act 2000, s.43 & s.66.** This policy provides authorisation for good-faith research under s.43, which converts otherwise unauthorised access into authorised access for the limited purpose of security testing.

9. Contact

- **Primary:** security@digitaliisla.co.in — monitored 24×7 by on-call.
- **Grievance Officer** (under DPDPA 2023): grievance@digitaliisla.co.in · +91 93145 91361.
- **Public key:** **Planned Q1 2027** .

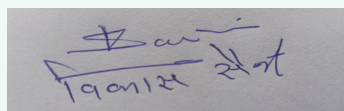
RESPONSIBLE DISCLOSURE COMMITMENT · SIGNED

Digitaliisla Technologies Private Limited commits to the safe-harbour above for every good-faith security researcher. We will acknowledge, triage, fix, and credit on the timelines stated. We will not pursue legal action against a researcher who follows this policy, and we will not weaponise this platform or its contracts against the people who help us keep it safe. When the law requires us to report upwards — to CERT-In, to IRDAI, to the Data Protection Board — we will, and we will not reveal the researcher's identity without consent.



Mrs. Monika Sharma

Director · Authorised Signatory



Mr. Vikas Saini

Director & Founder

Dated: 25 October 2026 · Jhunjhunu, Rajasthan, India

Witnessed by Grievance Officer: Mr. Alok Sharma, Advocate — Grievance Officer; Bar Council of Rajasthan, Enrolment No. R/1387/2012 · grievance@digitaliisla.co.in · +91 93145 91361

CIN U62011RJ2026PTC119030 · Registered office: Khemi Sati Road, Jhunjhunu, Rajasthan – 333001 · legal@digitaliisla.co.in