

AUDIT READINESS & REGULATORY COOPERATION STATEMENT

We're **built for inspection**. Any insurer, any regulator, any auditor — here's how we open the books.

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

Digitaliisla Technologies Private Limited operates in a regulated space (motor insurance survey, under IRDAI). We maintain documented, standing audit readiness — so insurer customers, government regulators, statutory auditors, and third-party assessors can verify our data-protection, security, and operational posture quickly and without disruption.

This page is a **single reference** for every audit stakeholder: who may audit, what we provide, how long it takes, and the standing cooperation commitment signed by the Board.

1. Who may audit DigiSurvey

Audit stakeholder	Basis	Typical scope	Standing right
Insurer customer (legal / infosec / internal audit)	DPA Clause 10 (audit right); MSA	Data handling, access logs, security controls, sub-processor arrangements, incident records, destruction evidence	Annual · 30-day notice · free
IRDAI (Insurance Regulatory and Development Authority of India)	IRDAI Act 1999, s.14(2); IRDAI (Surveyors) Regulations 2015	Surveyor-firm licence compliance; records of claims surveyed; IRDAI retention compliance; grievance handling	Statutory · immediate
Data Protection Board of India (DPBI)	DPDPA 2023, s.27(1)(d); s.33 (inquiry); s.36 (powers)	Processing records, grievance log, breach register, consent records, Data Fiduciary obligations	Statutory · immediate

Audit stakeholder	Basis	Typical scope	Standing right
CERT-In (Indian Computer Emergency Response Team)	IT Act 2000 s.70B; CERT-In Directions 28 April 2022	Cyber-incident logs (180-day retention), vulnerability-disclosure records, incident reports	Statutory · immediate
Statutory financial auditor (Company auditor appointed under Companies Act 2013)	Companies Act 2013, s.139 & s.143	Books of account, financial statements, tax computations, related-party transactions	Annual · statutory
GST authorities (Central / State)	CGST Act 2017, s.65 (audit); s.67 (inspection)	GST returns, tax invoices, input tax credit, electronic cash/credit ledger	Statutory · 15-day notice
Income Tax authorities	Income-tax Act 1961, s.133A (survey); s.142(2A) (special audit)	Books, bank records, salary / contractor payments, TDS compliance	Statutory · as served
MCA / ROC (Ministry of Corporate Affairs / Registrar of Companies)	Companies Act 2013, s.206 (inspection), s.212 (investigation)	Statutory registers, board resolutions, filings, beneficial ownership	Statutory · as served
Independent third-party assessor (SOC 2 / ISO 27001 auditor)	Our own engagement (SOC 2 Type I — target Q4 2027; SOC 2 Type II — target Q4 2028; ISO 27001 — target 2028.)	Control testing, evidence sampling, interviews	Planned
Penetration tester (external, qualified vendor)	Our own engagement	Web + API + mobile pen-test; social engineering out of scope by default	Planned Q1 2027

Audit stakeholder	Basis	Typical scope	Standing right
Security researcher (responsible disclosure)	Our Responsible Disclosure policy (planned); good-faith research	Vulnerability discovery, disclosure to security@digitaliisla.co.in, Hall of Fame	Always welcome

2. What we provide during an audit

Depending on scope, the auditor receives (through a secure data-room; nothing emailed in cleartext):

- **Access logs** — timestamped, actor-attributed, filterable by tenant / endpoint / time window.
- **Processing register (RoPA)** under DPDPA 2023 — complete record of processing activities.
- **Sub-processor list + their SOC 2 reports** — current certifications on file.
- **Breach register** — every reportable incident with timeline, root-cause analysis, remediation evidence.
- **Policy pack** — Privacy, DPA, Security Statement, Breach SOP, Data Retention, Zero-Commercial-Use Pledge, both Data Commitments.
- **Board resolutions** — signatory authority, Grievance Officer appointment, DPO (if designated), security governance.
- **Grievance log** — DPDPA grievances received, acknowledgement time, resolution time, action taken.
- **Infrastructure diagrams** — data flow, encryption boundaries, tenant isolation.
- **Destruction / return evidence** — for insurers off-boarding, cryptographic erasure records.
- **Employee security records** — NDA execution, access review, background check attestation (as applicable).
- **Insurance evidence** — Directors & Officers (D&O) and Cyber Liability policy certificates (limits available on NDA).

3. Standing timelines

Audit type	Our response SLA	Who leads from our side
Insurer customer audit (DPA Clause 10)	Acknowledge in 48 hours; data-room access within 5 business days of signed audit scope	Grievance Officer + Director (Mrs. Monika Sharma)

Audit type	Our response SLA	Who leads from our side
DPBI / CERT-In statutory notice	Acknowledge within 24 hours; substantive response as per the notice	Grievance Officer + Director (Vikas Saini)
IRDAI notice (surveyor-firm compliance)	Immediate — Grievance Officer coordinates with the Company's designated IRDAI-licensed surveyor engaged for the matter	Grievance Officer + Director (Mrs. Monika Sharma)
Income Tax / GST survey or notice	As statutorily served; CA / tax counsel engaged within 1 business day	Director (Mrs. Monika Sharma) + statutory auditor
MCA inspection	As statutorily served; Company Secretary / Director coordinates	Director (Mrs. Monika Sharma)
Independent security researcher	Acknowledge within 24 hours of email	Security team (security@digitaliisla.co.in)

4. What we do *not* provide (and why)

- **Other insurers' data** — strictly isolated. An insurer audit can only see that insurer's own tenant.
- **Source code (fully)** — except under a specific SOW with signed NDA; limited walk-through is normal, full source dump is not.
- **Live production access to auditors** — evidence is produced in sanitised exports; direct database access is not granted. (Replica / staging access on request with insurer sign-off.)
- **Personal information of our employees** beyond what is required for the specific audit scope.
- **Trade secrets** — prompt engineering, ML tuning parameters, pricing analytics methodology — outside the audit scope by default.

5. Audit cost

- **Insurer customer, annual, in-scope:** no cost to the insurer. Our effort absorbed.
- **Insurer customer, additional / incident-triggered:** no cost if the incident was our fault; otherwise at reasonable cost.

- **Statutory audits (IRDAI, DPBI, CERT-In, Income Tax, GST, MCA):** our standing obligation; no cost sought from any party.
- **Independent third-party assessor (SOC 2, ISO 27001):** our cost (part of our planned certification roadmap).

6. Cross-reference to specific regulatory items

- **DPDPA 2023** — our full compliance mapping is embedded in the Privacy Policy and DPA. The Record of Processing Activities (RoPA) is maintained internally and shared with regulators on notice.
- **CERT-In Direction 28 April 2022** — we maintain the required 180-day log retention; synchronise clocks to NIC NTP; mandatory 6-hour incident reporting; portal registration complete **In progress**.
- **IRDAI (Surveyors and Loss Assessors) Regulations 2015** — the Company's survey outputs are signed off by qualified, IRDAI-licensed professionals as required under the regulations; firm-level compliance records available on request.
- **Information Technology Act 2000, s.43A & SPDI Rules 2011** — reasonable security practices documented in the Security Statement; superseded by DPDPA 2023 but still a reference.
- **Companies Act 2013** — statutory auditor appointment on record; books of account maintained for 8 years.
- **GST Act 2017** — registered under GSTIN; monthly / quarterly returns on time.
- **Income-tax Act 1961** — TDS / TCS compliance; Form 26AS reconciliation.

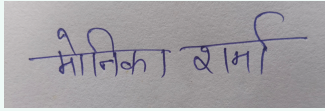
7. How to initiate an audit

- **Insurer customers (DPA audit right):** email legal@digitaliisla.co.in with the audit scope. We acknowledge in 48 hours and share the data room within 5 business days of agreed scope.
- **Government regulators:** serve the notice to our registered office (Khemi Sati Road, Jhunjhunu, Rajasthan – 333001) and email a copy to legal@digitaliisla.co.in. We will not require re-service.
- **Security researchers:** email security@digitaliisla.co.in. Good-faith research under the responsible-disclosure principles is welcomed and legally safe-harboured by us.

AUDIT COOPERATION COMMITMENT · SIGNED

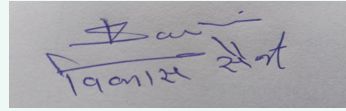
Digitaliisla Technologies Private Limited commits to **full and timely cooperation** with every lawfully constituted audit of its data-handling, security, financial, and operational practices — whether initiated by an insurer customer under contractual rights, by a government regulator under statutory authority, or by an

independent assessor under our own certification programme. We will not obstruct, delay, or scope-narrow an audit beyond what is objectively necessary to protect third-party privacy or trade secrets. Any evidence sought by a competent authority will be produced completely, truthfully, and promptly.



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