Security & Service Reliability Statement

Vidyaluma — A product of KRAVIA PRIVATE LIMITED

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

T01 · Version 1.0.0

The security, incident, access and recovery standards required for Vidyaluma, with evidence-based public claims.

On this page

1. Scope and assurance status
2. Identity, roles and school isolation
3. Information protection and secret handling
4. Workforce and supplier safeguards
5. Secure development and release controls
6. AI, identity and signing security
7. Incident management and notification
8. Reliability, backups and continuity
9. Independent assessment and transparency

▶ On this page

1. Scope and assurance status

1.a — Product. This Statement describes the security and reliability requirements for Vidyaluma, a product of KRAVIA PRIVATE LIMITED. It covers protected school information, public request paths, relevant integrations and the authorized workforce operating them. School-managed settings do not replace server-side protection of records.

1.b — Evidence boundary. Required controls are not proof that every control has been implemented or independently audited. Public statements must identify the relevant service/build, verified measures and material limitations. KRAVIA must not describe a provider's certificate as Vidyaluma's certification or claim 100% security, uninterrupted availability or zero possible data loss.

2. Identity, roles and school isolation

Skip to content

2.a — Authorization. Protected operations require authenticated users, valid school membership and server-side permission checks for the requested object and action. A school ID in a URL, a hidden button or a client-selected role is not sufficient protection. Cross-school requests are denied and tested, including exports, search, reports and background jobs.

2.b — Privileged accounts. Founder, support, infrastructure and school-administration privileges require stronger authentication, appropriate MFA, least privilege and review. Elevated access is purpose-limited and revoked when no longer needed. Role changes and departures must terminate relevant sessions and remove stale service access.

2.c — Recovery and disputes. Recovery verifies the appropriate person's identity and authority without collecting reusable secrets. Disputed school control leads to restricted sensitive changes and independent authority review. Emergency access requires recorded reason, limited scope, oversight and subsequent review; it is not a permanent bypass.

3. Information protection and secret handling

3.a — Encryption and access. Information needs appropriate encryption in transit and at rest, with controlled key and secret access. Protection is verified for actual databases, object stores, backups and provider connections. Saying "encrypted" must not obscure an unprotected endpoint, insecure export or broadly available decryption key.

3.b — Minimal logs. Logs record necessary technical events, school/user references, actions, outcomes and approvals while minimizing content. Passwords, OTPs, access tokens, signing links, raw Aadhaar payloads and full student documents must not be routinely logged. Sensitive incident evidence has a separate justified restricted store.

3.c — Uploaded and exported files. File handling applies appropriate type, size, integrity and malicious-content checks, scoped access and expiry. Export access is authenticated and auditable. Public storage paths or unbounded signed links must not expose school records to unrelated recipients.

4. Workforce and supplier safeguards

4.a — Personnel. Employees and contractors need confidentiality commitments, relevant training and approved role-based access. Support access is limited to the reported task and appropriately audited. A support ticket is not permission to browse an entire school or send its information to an unreviewed AI service.

4.b — Misuse response. Suspected employee misuse requires prompt containment, preservation of evidence, independent review and proportionate employment/contract measures, together with required incident notifications. Restricting a person's access does not replace fixing an enabling technical defect.

4.c — Providers. Actual service providers receive due diligence, appropriate agreements, restricted data and monitoring. New AI, hosting or communications providers must be reviewed before egress. T06 identifies the disclosure requirements; government interfaces and independent signing/payment roles are not all automatically classified as subprocessors.

5. Secure development and release controls

5.a — Changes. Relevant changes receive code review, tests, dependency and secret checks and appropriate security/privacy assessment. Development environments use synthetic or minimized data. A passing unit test cannot establish production consent, provider authorization, identity integrity or delivery behavior.

Skip to content

5.b — Policy protection. All Legal and Trust content is immutable through websites, apps, portals, CMS and application APIs. Authorized source changes require review, Founder approval for the exact release, tests and a controlled deployment. Hashes and source history detect changes but require protected approvals and deployment credentials to provide meaningful enforcement.

5.c — No false recovery. Teams must not weaken tests, delete genuine operational records, remove audit evidence or fabricate successful provider responses to clear a release gate. A production failure is resolved against preserved evidence with verified recovery and rollback boundaries.

6. AI, identity and signing security

6.a — AI controls. Tenant-bound retrieval, source authorization, no-training requirements, output review and privacy-preserving audit records apply to AI. Tool actions require permitted scopes and explicit human approval for consequential operations. Deletion and source revocation must propagate to retrieval indexes and caches.

6.b — Verification controls. OVSE identity, DigiLocker document consent/integrity, school-authority review and Leegality signing are distinct controls. Invalid state, wrong school, replay, withdrawn consent or a failed callback check must not activate a school. Access codes and provider secrets stay server-side.

6.c — Signing artifacts. Executed PDFs and audit evidence require integrity checks, access restrictions and justified retention. A disputed artifact is preserved as evidence rather than edited in place. Extra provider collection must match the configured transaction disclosure.

7. Incident management and notification

7.a — Response. KRAVIA evaluates suspected compromise, contains affected access, preserves relevant evidence and coordinates responsible technical, privacy and legal review. Severity depends on affected services, information, users and likely harm, not merely the number of support complaints.

7.b — Notifications. Applicable statutory, contractual and provider deadlines are tracked separately with their correct trigger and recipient. KRAVIA promptly informs affected schools, assists their notifications and meets its own obligations. A required initial report must not wait for every forensic detail to be complete.

7.c — Public updates. Service status and incident summaries reflect verified information, affected functions and recovery progress. They exclude personal data, private forensic records and exploitable technical detail. "Monitoring unavailable" is not displayed as "all operational".

7.d — Closure. Closure requires root-cause assessment, appropriate remediation, integrity checks, recovery verification, necessary notices and tracked preventive actions. Lessons inform tests and controls. T08 provides the private vulnerability-reporting route.

8. Reliability, backups and continuity

8.a — Backup governance. Critical records require protected backups and documented restore procedures. The recorded direction is quarterly backup restore tests and an annual disaster-recovery exercise. Actual schedules and results must support any public claim that these activities occur.

8.b — Recovery objectives. Recovery Time Objectives and Recovery Point Objectives are defined for relevant services from tested capability and accepted commitments. They are not invented as universal numbers. Recovery must preserve school isolation, legitimate transactions and deletion/legal-hold rules and must assess inconsistent provider callbacks or duplicate jobs.

Skip to content

8.c — Maintenance and outages. Planned work seeks low-impact windows and appropriate notice; urgent repairs may precede notice when justified. L08 governs support and L07 governs applicable commercial remedies. External failure does not automatically excuse KRAVIA's configuration, oversight, communication or reasonable recovery obligations.

9. Independent assessment and transparency

9.a — Assessments. Risk-based independent testing, vulnerability remediation and appropriate assurance reviews support the security program. Material defects receive accountable owners and remediation evidence. Certification is stated only for a verified current scope; an assessment plan is not a completed audit.

9.b — Controlled assurance. Schools may request relevant security information through support@vidyaluma.in. Sensitive reports may require authorization and confidentiality controls, but these must not obstruct legally or contractually required assurance. No source keys, customer records or private infrastructure secrets are published in the Trust Centre.

9.c — Review. This Statement is reviewed at least annually and after material incidents, legal changes, provider changes or infrastructure changes. Approved amendments use the read-only policy source-release process. The real publication date remains distinct from the intended policy-set date.

Related documents
L01 — Privacy PolicyL08 — Support & Service Commitments PolicyL09 — Data Processing AgreementT03 — Responsible AI PolicyT06 — Subprocessor & International Processing NoticeT07 — Data Retention, Export & Deletion PolicyT08 — Vulnerability Disclosure Policy

The current published version is shown. Earlier review copies do not create customer acceptance or contractual terms.

Vidyaluma

VidyaLuma

Clear school work, calmer daily decisions, and trusted records in one connected place.

Book a walkthrough

Contact support

Explore

About

Product

Pricing

School support

Book a walkthrough

Contact

Verify partner ID

Trust

Security & Service Reliability Statement

Legal

Privacy Policy

Terms & Conditions

Skip to content

Guides

Release notes

FAQs

Status

Student & School Data Protection Notice

Responsible AI Policy

Data Use & Purpose Limitation Statement

School Control, Access & Sharing Statement

Subprocessor & International Processing Notice

Data Retention, Export & Deletion Policy

Vulnerability Disclosure Policy

Cookie & Tracking Technologies Policy

Acceptable Use Policy

Disclaimer

Accessibility Statement

Billing, Subscription, Cancellation & Refund Policy

Support & Service Commitments Policy

Data Processing Agreement

Grievance, Complaints & Appeals Policy

School-controlled sharing **Role-aware access** **GST included in public pricing**

Built for school teams that need clear, trusted operations. Made in India, with love ❤ Copyright 2026 Vidyaluma. All rights reserved.

Legal Trust Privacy request Delete an account Service status Cookie choices Back to top ↑