Vulnerability Disclosure Policy

Vidyaluma — A product of KRAVIA PRIVATE LIMITED

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

T08 · Version 1.0.0

Private reporting, safe research boundaries, coordinated investigation and disclosure.

On this page

1. Purpose and scope
2. Reporting channel
3. Safe behavior
4. What makes a useful report
5. Triage and remediation
6. Coordinated disclosure and recognition
7. Privacy, incidents and complaints
8. Policy integrity

▶ On this page

1. Purpose and scope

1.a — Product. KRAVIA PRIVATE LIMITED welcomes good-faith reports of potential vulnerabilities affecting Vidyaluma systems that KRAVIA owns or is authorized to operate. This Policy provides a reporting process; it is not unlimited permission to test production, other schools, provider services or unrelated KRAVIA products.

1.b — Authorization boundary. Any active testing beyond ordinary authorized use needs the applicable explicit written scope and rules of engagement. A domain containing the brand name, a linked provider or an accessible resource does not establish authorization. Ask before testing when scope is uncertain.

2. Reporting channel

2.a — Private report. Send a concise initial report to support@vidyaluma.in with the subject "Security vulnerability — Vidyaluma" or use the approved private security-report route when available. State the affected

function, approximate time, safe reproduction steps, expected versus observed behavior and a contact method if follow-up is desired.

2.b — Sensitive evidence. Do not include reusable credentials, OTPs, full Aadhaar details, student records, unredacted private report/signing links or harmful payloads in an ordinary email. Request a protected evidence channel when necessary. A screenshot should be minimized and redacted before sharing.

2.c — No prerequisites for a concern. A person need not buy a plan to report a security issue. A lack of account access may limit investigation or action on protected information, but must not automatically prevent receipt of a general report.

3. Safe behavior

3.a — Minimize impact. Prefer a designated test environment and synthetic accounts/data under an agreed scope. Do not access, download, modify or disclose another person's information. If unexpected access occurs, stop, retain only the minimum safe evidence and report promptly.

3.b — Prohibited activity. Denial-of-service, resource exhaustion, credential stuffing, phishing, social engineering, malware, extortion, persistent access, destructive tests and attempts to bypass another school's boundaries are not authorized by this Policy. Do not create real charges, initiate signatures or trigger government-identity checks for an unaware person.

3.c — Provider systems. UIDAI/OVSE, DigiLocker, Leegality, payment and hosting services have their own authority and reporting arrangements. Vidyaluma cannot grant permission to test those systems. A report of a suspected integration defect should identify the boundary without extending testing into a provider account or service.

4. What makes a useful report

4.a — Reproducibility. Include the affected route or app feature, the account role and environment used, safe request/response observations and the limited impact demonstrated. Distinguish an actual data disclosure from a suspected risk. Avoid assertions of compromise based only on a scanner's severity label.

4.b — Data boundaries. For cross-school or access-control concerns, use only authorized synthetic evidence. Do not enumerate real students or schools to estimate the size of a problem. KRAVIA will investigate scope through controlled authorized systems.

4.c — Preservation. Necessary report evidence is preserved with access restrictions and integrity controls. Researchers should not retain or distribute school information beyond the authorized purpose. Coordinate secure deletion of inadvertently obtained information once evidence needs are resolved.

5. Triage and remediation

5.a — Assessment. KRAVIA records the report, assigns appropriate ownership and evaluates exploitability, affected information, school impact and required containment. A scanner result, duplicate report or disputed conclusion is reviewed proportionately rather than automatically dismissed.

5.b — Response expectations. Acknowledgement, update and remediation targets must reflect actual staffing and risk; this Policy creates no unsupported fixed patch deadline or continuously staffed bounty service. Critical incidents are escalated under T01 and applicable legal/provider deadlines are handled separately.

5.c — Remediation. Appropriate action may include access restriction, configuration or code correction, key/session revocation, provider coordination, recovery testing and affected-party notice. A fix is verified against

Skip to content

the issue and regressions. Legitimate audit records must not be destroyed merely to conceal the vulnerability.

6. Coordinated disclosure and recognition

6.a — Timing. Coordinate publication so affected people and systems are protected and verified remediation can occur. Do not publish secrets, school records or usable private links. KRAVIA should communicate progress and cannot demand indefinite silence simply to avoid embarrassment or prevent lawful reporting.

6.b — Researcher protection. Good-faith reporting itself must not result in retaliation by KRAVIA. Any specific legal safe-harbor or active-testing authorization requires an approved written scope; this Policy cannot bind governments, schools or third parties or promise immunity from their laws and rights.

6.c — Rewards and acknowledgement. No monetary bounty is promised unless a separate approved program states eligibility and terms. Public recognition requires appropriate agreement and must not expose a reporter who requests privacy. A reward dispute does not justify extortion or release of personal information.

7. Privacy, incidents and complaints

7.a — Report data. Contact details and necessary evidence are used for triage, investigation, coordination and justified accountability. Access is restricted and retention follows T07. We avoid collecting unrelated researcher information or using a security report as marketing consent.

7.b — Incident duties. A vulnerability may require an incident assessment and notifications even before the full root cause is established. KRAVIA meets its own obligations and assists affected schools. Public summaries are limited to verified, customer-safe information.

7.c — Escalation. Concerns about report handling may be escalated under L10. Applicable rights to contact a competent authority remain. A disputed technical assessment should receive meaningful review by an appropriate person.

8. Policy integrity

8.a — Review and approval. This Policy is reviewed at least annually and after material changes to reporting scope or service controls. It requires authorized legal/security review and Founder approval before publication. Changes are made through controlled source releases, not product interfaces.

8.b — Actual dates. The 1 November 2026 effective date does not retroactively authorize past testing, create a past bounty program or imply earlier acceptance of these rules. The actual approved version and publication record govern the notice supplied to a researcher.

Related documents
L01 — Privacy PolicyL04 — Acceptable Use PolicyL08 — Support & Service Commitments PolicyL10 — Grievance, Complaints & Appeals PolicyT01 — Security & Service Reliability StatementT07 — Data Retention, Export & Deletion Policy

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

Skip to content

VidyaLuma

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

Book a walkthrough **Contact support**

Explore

About
Product
Pricing
Guides
Release notes
FAQs

School support

Book a walkthrough
Contact
Verify partner ID
Status

Trust

Security & Service Reliability Statement
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

Legal

Privacy Policy
Terms & Conditions
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 ↑