Vendor/Contractor Data Incident Notification and Response Policy

1. Purpose and Scope

This Policy establishes the obligations of any vendor, contractor, or other counterparty ("Vendor") that accesses, processes, or stores Edulog Data with respect to the identification, containment, notification, and remediation of any actual or reasonably suspected Security Incident. This Policy is incorporated by reference into each agreement between Edulog and a Vendor that references it (each, the "Agreement"). This Policy supplements, and does not replace, any data security, privacy, or confidentiality obligations in the Agreement. In the event of a conflict between this Policy and the Agreement, this Policy controls with respect to Security Incident response. Edulog may update this Policy from time to time by posting a revised version at its designated URL; the version in effect at the time of a Security Incident governs.

2. Definitions

Term	Definition
Edulog Data	Any data, information, or records—including Personal Data, student transportation records, district client data, system configuration data, API credentials, and any other nonpublic business information—provided by Edulog to Vendor or to which Vendor is granted access under the Agreement.
Personal Data	Any information that identifies, relates to, or could reasonably be linked to an identified or identifiable natural person, including names, addresses, dates of birth, government identification numbers, financial account information, and for K–12 contexts, student education records as defined under FERPA and applicable state law.
Security Incident	Any actual, suspected, or reasonably threatened (i) unauthorized access to, acquisition of, use of, disclosure of, modification of, or destruction of Edulog Data; (ii) loss or theft of devices or media containing Edulog Data; (iii) ransomware, malware, or other cyberattack affecting systems that process or store Edulog Data; or (iv) any event that triggers a notification obligation under applicable law.
Vendor Systems	Any hardware, software, networks, cloud infrastructure, subprocessors, or other computing environments operated or used by Vendor in connection with the Agreement.
Containment	All steps taken to limit or stop the ongoing exposure, exfiltration, destruction, or corruption of Edulog Data following identification of a Security Incident.
Remediation	Corrective measures applied to Vendor Systems and processes to eliminate the root cause of a Security Incident and reduce the likelihood of recurrence.

Regulatory Deadline	Any legally mandated timeframe for notification or reporting imposed by applicable state or federal law (e.g., state breach notification statutes, FERPA), which may be shorter than the contractual deadlines in this Policy.

3. Notification Obligations

Vendor shall notify Edulog of any Security Incident as soon as practicable and in no event later than 48 hours after Vendor first becomes aware, or reasonably suspects, that a Security Incident has occurred. The 48-hour deadline is not contingent on Vendor completing its investigation or confirming the incident—reasonable suspicion is sufficient to trigger this obligation. Notice shall be provided simultaneously to:

Role	Contact
General Counsel	legal@edulog.com
Executive Director, Technology & Security	security@edulog.com
Incident Response	ninox@edulog.com

Initial notice shall include, to the extent then known: (i) date and time of first detection; (ii) nature of the incident; (iii) categories and approximate volume of Edulog Data potentially affected; (iv) Vendor systems involved; (v) immediate containment measures taken or in progress; (vi) contact information for Vendor's incident response lead; and (vii) whether the incident is ongoing. Vendor shall supplement notice promptly as additional information becomes available. Incomplete initial notice does not excuse the 48-hour deadline.

4. Response Timeline

Trigger	Deadline	Obligation
Security Incident suspected or detected	48 hours	Written notice to all Edulog contacts below
Initial notice delivered	72 hours	First status update; confirm containment
Ongoing until contained	Every 72 hours	Written status updates
Containment confirmed	30 days	Final incident report

Deadlines that fall on a weekend or federal holiday are not extended. Time is of the essence with respect to all notification obligations in this Policy.

5. Containment and Cooperation

Upon identification of a Security Incident, Vendor shall immediately take all reasonable steps to contain the incident, including: (i) isolating affected systems; (ii) preserving logs and forensic evidence; (iii) revoking or rotating compromised credentials, API keys, and tokens; (iv) suspending third-party access connected to the incident; and (v) engaging qualified incident response personnel.

Vendor shall provide Edulog and its designated representatives with timely access to Vendor's incident response personnel and, upon request, to relevant logs, forensic reports, and remediation evidence. Vendor shall respond to Edulog inquiries within 4 business hours during active investigation, and shall not make any public statement, press release, or regulatory filing regarding a Security Incident involving Edulog Data without Edulog's prior written consent, except to the extent prohibited by law.

Vendor shall not destroy, overwrite, or dispose of any systems, logs, media, or data relevant to a Security Incident without Edulog's prior written consent during any investigation, litigation hold, or regulatory inquiry. This obligation survives termination of the Agreement.

6. Final Incident Report

Within 30 days of full containment, Vendor shall deliver a written final incident report covering: (i) incident timeline from detection through containment and remediation; (ii) root cause analysis; (iii) scope of Edulog Data affected; (iv) categories of individuals whose Personal Data was involved and approximate count; (v) all containment and remediation steps taken; (vi) any subprocessors involved; (vii) regulatory or law enforcement notifications made; (viii) residual risk assessment; and (ix) a corrective action plan with milestones and owners. The final report is Edulog Confidential Information.

7. Remediation

Vendor shall implement all remediation measures identified in its final incident report and shall, at its own cost: (i) patch or replace affected systems within timeframes in the corrective action plan; (ii) conduct a post-incident penetration test or security audit by a qualified independent third party within 90 days of containment; and (iii) implement enhanced security controls reasonably requested by Edulog consistent with industry standards. Remediation obligations are in addition to any indemnification or damages obligations under the Agreement.

8. Regulatory Compliance

Vendor acknowledges that Edulog Data may include student education records subject to FERPA and data subject to applicable state breach notification laws. Vendor shall maintain awareness of applicable notification laws in jurisdictions where Edulog's district clients operate, provide Edulog with immediate notice if any Regulatory Deadline is shorter than the contractual deadlines in this Policy, and provide Edulog with copies of all regulatory or law enforcement notifications relating to Edulog Data within 24 hours of transmittal.

9. Cost Allocation

Unless otherwise agreed in writing, Vendor shall bear all costs associated with: (i) investigation, containment, and remediation of any Security Incident arising from or attributable to Vendor's systems, personnel, or subprocessors; (ii) required regulatory notifications; (iii) credit monitoring or identity protection services required by applicable law or reasonably requested by Edulog; (iv) post-incident security audits; and (v) any fines or penalties attributable to Vendor's acts or omissions.

10. Subprocessors

Vendor shall ensure that any subprocessor accessing, processing, or storing Edulog Data is contractually bound to security incident notification and response obligations at least as protective as those in this Policy. Vendor remains fully responsible to Edulog for its subprocessors' acts and omissions. Vendor's notification obligations are triggered from the date Vendor first becomes aware of a subprocessor's incident.

11. Recordkeeping

Vendor shall maintain complete records of all Security Incidents (including incidents investigated but not confirmed) for a minimum of 5 years, including all notices, forensic reports, remediation documentation, regulatory filings, and corrective action plans. Vendor shall make such records available to Edulog within 5 business days of request. This obligation survives termination of the Agreement.

12. Remedies

The obligations in this Policy are material terms of the Agreement. Vendor's failure to comply with notification deadlines or other obligations in this Policy constitutes a material breach of the Agreement. Nothing in this Policy limits Edulog's right to seek injunctive or other equitable relief without bond. The rights and remedies in this Policy are cumulative with those in the Agreement and at law or equity.

Sample Incorporation-by-Reference Clause

The following language may be inserted into any Edulog vendor or contractor agreement to incorporate this Policy by reference:

"Vendor shall comply with Edulog's Data Incident Notification and Response Policy, available at www.edulog.com, as updated from time to time (the 'Incident Response Policy'). The Incident Response Policy is incorporated herein by reference and made a part of this Agreement. Capitalized terms used in the Incident Response Policy and not defined therein have the meanings given in this Agreement."

Last updated: April 19, 2026