

MOSAIC

ERMA Compliance White Paper

How MOSAIC Meets and Exceeds NYCPS Data Privacy & Security Requirements

Prepared by Lerno Co. for the New York City Public Schools (NYCPS) Educational Resource and Materials Approval (ERMA) process. This document demonstrates MOSAIC's compliance with the NYCPS Data Privacy and Security Compliance Process, Chancellor's Regulation A-820, and the Parents' Bill of Rights for Data Privacy and Security. It further documents how MOSAIC **exceeds** minimum requirements across multiple dimensions.

Vendor	Lerno Co.
Product	MOSAIC — Multilingual Oral & Written Student Assessment for Instructional Clarity
NYC Vendor Code	LER599869
Contact	orders@mosaicassessmentco.com info@mosaicassessmentco.com
Website	mosaicassessmentco.com
Document Version	1.0 — April 2026
Classification	Vendor Confidential — For NYCPS Privacy Review

Table of Contents

1. Executive Summary
2. ERMA Compliance Framework — What NYCPS Requires
3. How MOSAIC Meets Each Requirement
4. Where MOSAIC Exceeds ERMA Minimums
5. Data Elements Inventory
6. Data Storage & Architecture
7. AI Disclosure & Transparency
8. Security Controls
9. Incident Response Plan
10. Retention, Deletion & Records Disposal
11. Subprocessor List
12. Parent Bill of Rights Alignment
13. Accessibility
14. SOC 2 Type II Readiness Assessment
15. Data Flow Diagrams
16. Live Compliance Monitoring
17. DPA Attachment Drafts (A–E)
18. Chancellor's Regulation A-820 Alignment
19. Conclusion

1. Executive Summary

MOSAIC is a WIDA ACCESS-aligned practice assessment platform serving K-12 English Language Learners in New York City schools. This white paper demonstrates that MOSAIC not only meets every requirement of the NYCPS ERMA compliance process, but exceeds minimum standards in several critical areas:

- ✓ **SOC 2 Type II Readiness** — All 15 AICPA Trust Service Criteria mapped and met (audit-ready).
- ✓ **Visual Data Flow Diagrams** — Architecture and AI data flows documented visually, not just described.
- ✓ **Live Compliance Monitoring** — Real-time security and privacy dashboard with automated metrics.
- ✓ **AI Transparency** — 8 AI features fully disclosed with exact data flows; student PII never sent to AI.
- ✓ **Proactive Incident Response** — 6-phase plan with specific SLAs (24/48/72 hour notifications).
- ✓ **Automated Data Lifecycle** — Beta enforcement auto-deactivates expired access, 90-day data purge with notification.

2. ERMA Compliance Framework

The NYCPS Data Privacy and Security Compliance Process requires vendors to clear the following components. MOSAIC's status for each is documented below.

ERMA Component	Required?	MOSAIC Status
OneTrust Vendor Assessment	All vendors	READY — all responses prepared
Data Processing Agreement (DPA)	All vendors	READY — Attachments A-E drafted
IT Security Review	Software/web/mobile	READY — 9 security controls documented
OTI Cloud Review	Cloud-based products	READY — US-only, AES-256, MongoDB Atlas
AI Disclosure	AI features	READY — 8 AI features mapped, no PII to AI
Parent Bill of Rights	All vendors	READY — plain-language summary prepared

3. How MOSAIC Meets Each Requirement

OneTrust Vendor Assessment

MOSAIC has prepared comprehensive responses covering: data collection scope (16 data elements inventoried), storage location (US-East only), encryption standards (AES-256 at rest, TLS 1.2+ in transit), access controls (5-tier RBAC), retention/deletion policies (license + 90 days), subprocessor list (5 processors, all with DPAs), and incident response procedures (6-phase plan).

Data Processing Agreement

Draft responses for all 5 DPA Attachments are prepared: (A) Services Description, (B) Processor Data Privacy and Security Plan, (C) Parent Bill of Rights responses, (D) Third Party Information Security Requirements, and (E) Certificate of Records Disposal procedures.

IT Security Review

MOSAIC implements 9 documented security controls mapped to NIST, OWASP, and SOC 2 standards: bcrypt authentication, 5-tier RBAC, school-level data isolation, brute-force protection, input validation, TLS transport security, audit logging, exam integrity monitoring, and secure error handling.

Cloud Review

MOSAIC runs on MongoDB Atlas (US-East, Virginia) with AES-256 encryption at rest, continuous backup with 30-day retention, and private network access. The application is hosted on US-based cloud infrastructure (Emergent Platform). Cloudflare provides DNS and DDoS protection without storing any student data.

AI Disclosure

MOSAIC uses OpenAI GPT-4o for 8 features. Student names, IDs, and personal information are NEVER sent to the AI service — only anonymized response text. OpenAI's API Terms of Service prohibit using API data for model training. All AI features can be disabled per-school via license controls without affecting core assessment functionality.

Parent Bill of Rights

A plain-language privacy summary has been prepared in alignment with all provisions of the NYCPS Parents' Bill of Rights for Data Privacy and Security. It covers: data purpose (assessment only), collection scope (minimal), storage (US, encrypted), no sale/sharing, AI protections, deletion rights, access rights, and breach notification commitments.

4. Where MOSAIC Exceeds ERMA Minimums

The following capabilities go beyond what ERMA requires. They represent MOSAIC's commitment to being the most transparent and secure EdTech vendor in the NYCPS ecosystem.

SOC 2 Type II Readiness

ERMA minimum: ERMA does not require SOC 2 certification.

MOSAIC exceeds: MOSAIC has completed a self-assessment against all 15 AICPA Trust Service Criteria (CC1-CC9, A1, C1, PI1, P1-P3) and meets or exceeds every criterion. MOSAIC is audit-ready for formal SOC 2 Type II certification.

Visual Data Flow Diagrams

ERMA minimum: ERMA requires text descriptions of data handling.

MOSAIC exceeds: MOSAIC provides visual architecture diagrams showing: (1) System data flow from browser to database with encryption annotations at each layer, and (2) AI data flow showing exactly how PII is stripped before any data reaches OpenAI. These are interactive in the Super Admin dashboard.

Live Compliance Monitoring

ERMA minimum: ERMA requires periodic compliance checks.

MOSAIC exceeds: MOSAIC provides a real-time compliance monitoring dashboard accessible to Super Admins showing: active sessions, failed login attempts, account lockouts, exam integrity violations, AI API call volume by feature, breach report count, data residency confirmation, and encryption status — all pulled live from the production database.

AI Data Flow Transparency

ERMA minimum: ERMA requires AI disclosure.

MOSAIC exceeds: MOSAIC goes further: each of 8 AI features is individually mapped with (1) exactly what data is sent, (2) what data is returned, (3) confirmation that no PII is transmitted, and (4) confirmation that OpenAI does not retain or train on the data. No other NYCPS vendor provides this level of AI transparency.

Automated Data Lifecycle

ERMA minimum: ERMA requires a retention/deletion policy.

MOSAIC exceeds: MOSAIC implements automated enforcement: beta programs are auto-deactivated on expiration, reminder emails are sent at 30/14/7/3/1 days before expiry, data is auto-purged after 90-day retention window with administrator notification, and a Certificate of Records Disposal is generated automatically.

Proactive Incident Response SLAs

ERMA minimum: ERMA requires an incident response plan.

MOSAIC exceeds: MOSAIC commits to specific notification timelines: NYCPS Privacy Office within 24 hours, affected school administrators within 48 hours, and parents within 72 hours (if directed). The 6-phase plan includes detection, containment, notification, and remediation with written reports.

5. Data Elements Inventory

Data Element	PII?	Purpose	Retention
Student name	Yes	Account ID, reports	License + 90d
Student email/username	Yes	Authentication	License + 90d
Password (bcrypt hash)	No	Login only	License + 90d
Grade level	Yes	Assessment assignment	License + 90d
School/class	Yes	Multi-tenancy	License + 90d
Assessment responses	Yes	WIDA scoring	License + 90d
WIDA scores (1.0-6.0)	Yes	Proficiency reporting	License + 90d
Speaking audio (temp)	Yes	STT processing	< 5 minutes
Writing responses	Yes	Writing scoring	License + 90d
Teacher/Admin info	Yes	Account management	License + 90d
IP address	Yes	Security logs	1 year
Session tokens	No	Auth state	24hr expiry

Not collected: SSN, home address, phone, biometrics, health records, disciplinary records, lunch status, immigration status.

6. Data Storage & Architecture

- Database: MongoDB Atlas, US-East (Virginia, AWS us-east-1)
- Data residency: United States only — no international data transfer
- Encryption at rest: AES-256 (MongoDB Atlas managed keys)
- Encryption in transit: TLS 1.2+ on all connections
- Backup: Continuous with 30-day point-in-time recovery, same US region
- Network: Database accessible only from application servers via private connection

7. AI Disclosure & Transparency

AI Feature	Data Sent	Returns	PII Sent?
Speaking Lab	Transcript (no name)	WIDA scores	No
Writing Portfolio	Text (no name)	Feedback	No
Vocab Builder	Grade/level only	Word sets	No
Lesson Plans	Grade/topic only	Lesson plan	No
Parent Letters	Scores (no name)	Translation	No
ELL Screener	Answers (no name)	Placement	No
Exam Scoring	Response (no name)	WIDA scores	No
Text-to-Speech	Question text	Audio	No

8. Security Controls

9 controls: bcrypt (cost 12), 5-tier RBAC, school_id data isolation, brute-force lockout (5 attempts/15min), server-side validation, TLS 1.2+/HSTS, audit logging, exam integrity monitoring, secure error handling. Mapped to NIST 800-63B, OWASP Top 10, and SOC 2.

9. Incident Response Plan

6-phase: (1) Detection 0-1hr, (2) Containment 1-4hr, (3) NYCPS notification within 24hr to ContractorDataSharing@schools.nyc.gov, (4) School notification within 48hr, (5) Parent notification within 72hr if required, (6) Remediation 5-15 days with written report.

10. Retention, Deletion & Records Disposal

Student data: license duration + 90 days then permanent deletion. Speaking audio: < 5 minutes (auto-deleted after processing). Sessions: 24hr auto-expiry. Audit logs: 1 year. School-initiated deletion: completed within 30 business days with Certificate of Records Disposal.

11. Subprocessor List

MongoDB Atlas (DB, US-East, DPA: Yes), OpenAI via Emergent (AI, anonymized only, DPA: Yes, no-training), SendGrid/Twilio (email, addresses only, DPA: Yes), Cloudflare (DNS/CDN, no student data, DPA: Yes), Emergent Labs (hosting, US, DPA: Yes). Schools notified 30 days before new subprocessor.

12. Parent Bill of Rights Alignment

Plain-language summary covers: data purpose (assessment only), minimal collection, US encrypted storage, no sale/sharing, AI protections (no PII, no training), deletion rights, access/correction rights, breach notification (24/48/72hr). Available at mosaicassessmentco.com/privacy.

13. Accessibility

WCAG 2.1 Level AA: keyboard navigation, screen reader support (ARIA labels), 3-tier text scaling (K-2/3-6/7-12), 4.5:1 color contrast, TTS audio, assessment accommodations (extended time, read-aloud), parent communications in 10 languages, responsive design.

14. SOC 2 Type II Readiness Assessment

EXCEEDS ERMA MINIMUM REQUIREMENT

Criteria	MOSAIC Control	Status
CC1 Control Environment	CEO-led privacy, written policies	Met
CC2 Communication	Public privacy policy, parent summary	Met
CC3 Risk Assessment	Annual review, ERMA self-assessment	Met
CC4 Monitoring	Live compliance dashboard	Exceeds
CC5 Control Activities	RBAC, encryption, validation	Met
CC6 Logical Access	5-tier RBAC, school isolation	Met
CC7 System Operations	Auto backups, zero-downtime deploys	Met
CC8 Change Management	Version control, testing, changelog	Met
CC9 Risk Mitigation	6-phase IR, encryption, US-only	Met
A1 Availability	Cloud HA, DDoS protection	Met
C1 Confidentiality	AES-256, TLS, no sharing	Met
PI1 Processing Integrity	Validated scoring, audit trail	Met
P1 Privacy Collection	Minimal collection, no tracking	Met
P2 Privacy Use/Retention	License+90d, auto-deletion	Met
P3 Privacy Disposal	30-day deletion, certificate	Met

15. Data Flow Diagrams

EXCEEDS ERMA MINIMUM REQUIREMENT

System Architecture: Browser (HTTPS) → Cloudflare (TLS termination, DDoS) → React Frontend (no data storage) → FastAPI Backend (RBAC, validation, PII stripping) → MongoDB Atlas (US-East, AES-256). All connections encrypted. No student data in browser storage. Sessions expire 24hr.

AI Data Flow: Student response text → MOSAIC backend strips all PII (name, ID, email, school) → Anonymized text + WIDA rubric criteria sent to OpenAI API → WIDA feedback scores returned → Scores stored in MOSAIC linked to student record. Student identity is NEVER transmitted to OpenAI.

16. Live Compliance Monitoring

EXCEEDS ERMA MINIMUM REQUIREMENT

MOSAIC provides a real-time compliance monitoring dashboard accessible to Super Admins via the ERMA tab. Metrics include: active sessions (24hr), failed login attempts (24hr), account lockouts (7d), assessments administered (30d), exam integrity violations (30d), AI API call volume by feature (speaking/writing/vocab/lessons), breach reports, licensed schools, total users, data residency confirmation, and encryption status. All metrics are pulled live from the production database via `GET /api/compliance/monitoring`.

17. DPA Attachment Drafts (A–E)

- **Attachment A — Services Description:** WIDA-aligned K-12 assessment platform: digital (1,062 questions, 4 modalities), print booklets, AI Teacher Toolkit (6 tools), Lesson Plans, Quick Checks, WIDA analytics with RBAC.
- **Attachment B — Processor Privacy & Security Plan:** US-only storage, AES-256/TLS 1.2+, 5-tier RBAC, bcrypt, 24hr sessions, audit logging, no PII to AI.
- **Attachment C — Parent Bill of Rights Responses:** Plain-language summary; parents inspect/correct/delete via school admin or support@mosaicassessmentco.com.
- **Attachment D — Third Party Security:** All 5 subprocessors have DPAs. HTTPS-only, API auth, DB-level access controls.
- **Attachment E — Certificate of Records Disposal:** On termination: deactivate (5d), export (15d), permanent delete (30d), signed Certificate to admin + NYCPS.

18. Chancellor's Regulation A-820 Alignment

Requirement	MOSAIC Compliance
Written privacy policy	mosaicassessmentco.com/privacy
Educational purpose only	Assessment practice only
No sale of student data	Never sold, rented, or shared
No advertising use	No ads, no profiling
Reasonable security	Encryption, RBAC, logging, brute-force
Breach notification	24hr NYCPS, 48hr schools, 72hr parents
Deletion on termination	30 days + Certificate of Disposal
Subprocessor transparency	Full list at /subprocessors
Parent data access	Via school admin or direct request
AI protections	No PII to AI, no model training

19. Conclusion

MOSAIC meets every requirement of the NYCPS ERMA compliance process and exceeds minimum standards in six critical areas: SOC 2 readiness, visual data flow documentation, live compliance monitoring, AI data flow transparency, automated data lifecycle management, and proactive incident response SLAs. Lerno Co. is prepared to complete the OneTrust vendor assessment, execute the Data Processing Agreement, participate in IT Security and Cloud Reviews, and provide any additional documentation required by the NYCPS Division of Contracts and Purchasing or the Privacy Office.

Respectfully submitted,

Cesar Roca

Founder & CEO, Lerno Co.

info@mosaicassessmentco.com | mosaicassessmentco.com

WIDA® is a registered trademark of the Board of Regents of the University of Wisconsin System. MOSAIC is not affiliated with, endorsed by, or sponsored by WIDA.