Kiteworks

Securing State, Local, and Education Data Exchange in the AI Era

Unifying Data Governance, AI Control, and Compliance Across Every Channel a SLED Organization Uses to Exchange Sensitive Data

Executive Summary

State, local, and education organizations hold some of the most sensitive personal data in the country -- citizen records, student information, criminal justice files, benefits applications, and health data -- under one of the most overlapping regulatory stacks of any sector. AI has moved into production across citizen services, casework, and classrooms ahead of the governance built to manage it. Auditors and regulators are now applying every existing framework -- CJIS, FERPA, HIPAA, IRS 1075, FedRAMP, StateRAMP, NIST 800-53/171, CMMC 2.0 -- to AI agent activity, without waiting for new rules.

Kiteworks closes the exposure at the data layer: one platform unifying email, file sharing, MFT, SFTP, data forms, APIs, and AI workflows under a single policy engine, audit log, and security architecture.

The Challenge

AI is in production across citizen services, casework, student support, and benefits administration. The data layer those workflows consume is the layer most agencies and institutions have not extended their governance to -- and the regulatory stack (CJIS, FERPA, HIPAA, IRS 1075, FedRAMP, StateRAMP, NIST 800-53/171, CMMC 2.0) already applies to every interaction with it, human or agent.

Most SLED organizations operate 5 to 10 separate tools for sensitive data exchange -- each with its own policies, audit logs, and gaps. When AI agents reach into all of those channels, fragmentation that was already a compliance liability becomes an AI governance crisis. When an auditor asks who authorized each AI interaction with regulated data, the answer becomes a multi-week investigation across fragmented logs and shared service accounts.

At a Glance

- **52% of U.S. K-12 school districts experienced a cybersecurity incident in 2025 -- up from 31% in 2023**[1]
- **90% of government organizations lack purpose binding controls for AI agents; 76% lack a kill switch**[2]
- **71% of government boards are not engaged on AI governance -- the worst of any sector**[2]
- **25% of government organizations reported a data breach in the past 12 months -- among the highest of any sector surveyed**[3]
- **75% of government respondents require FedRAMP for cloud workflows; 69% require FIPS 140-3**[4]
- **$2.28M average ransomware recovery cost in lower education in 2025**[5]

The Kiteworks Solution

Kiteworks is the secure data exchange for state, local, and education. One platform. One policy engine. One audit log. Built on a hardened virtual appliance with FIPS 140-3 validated cryptography, single-tenant isolation, and tamper-evident audit streamed in real time to the organization's SIEM.

Control

Policy-enforced access and complete attribution across email, file sharing, MFT, SFTP, data forms, APIs, and AI -- one auditor-ready record of every interaction with regulated data, human or agent. ABAC and RBAC enforce who can access what data under which conditions at the content layer, not just the network layer.

AI Governance

Through Kiteworks Compliant AI, including the Secure MCP Server, AI agents are cryptographically authenticated, bound to the human authorizer, and governed by attribute-based access on every request. Independent of model, vendor, or model-level guardrails. The delegation chain is preserved -- every AI access traces back to a specific human, policy, and timestamp.

Compliance

Pre-mapped to CJIS, FERPA, HIPAA, IRS 1075, FedRAMP, StateRAMP, NIST 800-53, NIST 800-171, CMMC 2.0, ISO 27001, and SOC 2. FedRAMP Moderate Authorized since 2017; FedRAMP High In Process. The full FedRAMP High control baseline (NIST 800-53 Rev 5) documented and assessor-ready. Evidence assembles in hours, not weeks.

Anticipated Outcomes

- **Unified governance.** Replace 5 to 10 fragmented tools with one control plane.
- **AI without compounding regulatory risk.** Authenticated identity, policy-enforced access, FIPS 140-3 encryption, and full audit applied to every AI workflow.
- **Audit trails auditors can read.** Real-time SIEM streaming with full attribution.
- **Evidence in hours, not weeks.** On-demand exports ready for CJIS, FERPA, HIPAA, IRS 1075, FedRAMP, StateRAMP, NIST 800-53/171, and CMMC examinations.
- **Sovereignty for state and local jurisdictions.** In-jurisdiction key custody, geofencing, and data residency.

Sources

[1] Clever, Cybersecure 2026 Report, March 2026.
[2] Kiteworks, Data Security and Compliance Risk: 2026 Forecast Report, December 2025.
[3] Kiteworks, Data Security and Compliance Risk: 2025 MFT Survey Report, 2025.
[4] Kiteworks, Data Security and Comwpliance Risk: 2025 Data Forms Survey Report, 2025.
[5] Sophos, State of Ransomware in Education, 2024.