Kiteworks

COMPLIANCE BRIEF

Compliance-ready AI With Kiteworks: Safeguarding Federal AI Implementation

Essential Security Controls for Executive Order Compliance

Executive Orders 13960 and 14179 and Memoranda M-25-21/22 establish frameworks for federal agencies to accelerate AI adoption while maintaining appropriate safeguards. Executive Order 13960 (December 2020) first outlined principles for trustworthy AI in government, while Executive Order 14179 and the memoranda (April 2025) removed bureaucratic barriers to responsible AI usage across all executive departments and agencies. Chief AI Officers must be designated within 60 days, with agency AI governance boards established within 90 days. Within 180 days, agencies must develop AI strategies and compliance plans, followed by policy updates within 270 days. After 365 days, agencies must implement risk management practices for high-impact AI use cases or discontinue noncompliant systems. Agencies failing to meet these requirements risk being unable to deploy AI technologies essential for government operations. The Kiteworks AI Data Gateway provides robust security, access control, and tracking features that create a secure bridge between AI systems and sensitive government data repositories, directly addressing requirements outlined in these orders.

Secure Data Control With Customer-owned Keys and Comprehensive Audit Logs

Federal agencies must implement robust contract closeout procedures for AI systems, ensuring proper data preservation and continued access when AI service contracts end. Memorandum M-25-22 requires agencies to work with vendors to maintain rights to data and derived products after contract termination, while also contributing to a shared repository of AI acquisition best practices. The Kiteworks AI Data Gateway supports these requirements through customer-owned keys, which gives agencies complete control over their encryption keys as sensitive data moves between repositories and AI systems. This ensures that neither Kiteworks staff nor government entities can access encrypted data without explicit permission. The platform's comprehensive audit logs with SIEM feeds maintain detailed records that document all data transfers between enterprise repositories and AI systems, supporting both compliance verification and best practice development. Kiteworks' tiered internal services with zero-trust principles architecture creates secure information boundaries that help maintain data integrity during vendor transitions, while detailed activity logs provide the necessary data for independent evaluations of data access patterns required by federal guidelines.

Solution Highlights

- Customer-owned keys
- Comprehensive audit logs with SIEM feeds
- Zero-trust data exchanges
- Hardened virtual appliance
- Double encryption

Internal Policy Implementation and Cybersecurity Alignment

Federal agencies must update their internal policies on IT infrastructure, data governance, cybersecurity, and privacy within 270 days as mandated by Memorandum M-25-21. These policies must align with Executive Orders 14179 and 13960, requiring robust security controls and protection mechanisms to safeguard sensitive government data as it flows to and from AI systems. The Kiteworks AI Data Gateway supports this compliance requirement through its comprehensive security architecture built on NIST CSF principles. The platform's role-based access controls (RBAC) and attribute-based access controls (ABAC) implement the least-privilege defaults essential for controlling who can access specific data repositories. Kiteworks' zero-trust data exchanges allow agencies to define and enforce dynamic security rules based on data sensitivity, user attributes, and actions, ensuring appropriate data handling as information moves between repositories and AI systems. The hardened virtual appliance with multiple protection layers, including embedded network firewall, web application firewall, and double encryption (both file-level and disk-level), provides the defense-in-depth strategy required by federal cybersecurity standards. These capabilities work together to create a secure data gateway that satisfies the updated policy requirements for secure AI data access.

Data Inventory, Tracking, and Monitoring for AI Implementation

Federal agencies must maintain comprehensive data inventories for AI systems as mandated by the OPEN Government Data Act and OMB Memorandum M-25-05. Chief AI Officers are responsible for ensuring all custom-developed AI code and training data are properly inventoried, shared, and maintained in agency repositories. Kiteworks' robust tracking capabilities create a complete audit log of all data exchanges between enterprise repositories and AI systems. The platform consolidates all compliance-relevant data into a single, searchable activity log that captures date, user, activity, IP address, and custom metadata as information flows through the gateway. This comprehensive tracking documents views, downloads, uploads, edits, emails, shared folders, and files, providing complete visibility into which AI systems access which data assets. Admin reporting tools generate both built-in and custom reports that function as detailed inventories of data movement between repositories and AI systems. The gateway's comprehensive audit logs with SIEM feeds ensure all data transfer activities are recorded without throttling, while integration with enterprise security systems via syslog or Splunk Universal Forwarder enables monitoring AI data access patterns across the organization.

The White House Executive Orders and Memoranda establish strict timelines and stringent requirements for federal agencies implementing AI systems. Kiteworks delivers the comprehensive security framework these agencies need to meet compliance deadlines and maintain operations. The platform's end-to-end encryption, granular access controls, and detailed activity tracking create a secure foundation for handling sensitive AI data throughout its life cycle. From initial development to contract closeout, Kiteworks protects data integrity while maintaining the transparency required by federal regulations. By implementing the Kiteworks AI Data Gateway, agencies can accelerate AI adoption with confidence, ensuring only authorized AI systems can access sensitive information while maintaining complete control over their data repositories. This powerful combination of security and governance features empowers agencies to harness AI innovations while protecting government information assets.

June 2025

www.kiteworks.com