Island

Solution Brief

AI Governance for California State Agencies

Executive Order N-5-26 | Trusted AI Procurement

How Island operationalizes AI governance for California's GenAI procurement mandate

SOC 2 Type 2 ISO 27001

The Challenge

California EO N-5-26: How Island Maps to Each Requirement

On March 30, 2026, Governor Newsom signed Executive Order N-5-26, directing state agencies to facilitate employee access to vetted GenAI tools with appropriate privacy and cybersecurity safeguards within 120 days. The order also requires new AI vendor certifications covering content safety, bias governance, and civil rights protections, and empowers California to separate its procurement standards from federal policy if needed.

Most agencies lack the tooling to operationalize these requirements. Island provides a single platform that makes compliance automatic, and is already SOC 2 Type 2 and ISO 27001 certified for processing sensitive government data.

Vetted GenAI Access & Shadow AI Discovery — EO §4(a)

Control which GenAI tools employees can access through browser-native allowlists, blocklists, and approval workflows. Detect unsanctioned AI usage across the organization in real time with risk scoring of 200K+ extensions. In-browser notifications automatically redirect employees to approved tools or display your agency's AI policy.

Privacy Safeguards & Data Loss Prevention — EO §4(a)

Enforce granular DLP policies that block PII, source code, financial data, and other sensitive categories from being shared with AI tools like ChatGPT. Prevent LLMs from training on employee prompts, including from personal accounts. Disable third-party connections and chat sharing within AI applications for surgical data control.

Cybersecurity Safeguards & Zero Trust — EO §4(a)

Browser-native protection against phishing, malware, and zero-day exploits without separate security tools. Zero Trust Network Access grants application-level access, not full network access, based on identity, device posture, and context. Block unauthorized AI browser extensions to prevent shadow AI from creating security gaps.

Transparency, Accountability & Audit — EO §§1, 3, 5

Maintain detailed audit logs of every AI interaction, including full chat history with AI tools. User behavior analytics with session recording, custom dashboards, and SIEM integration provide complete visibility for compliance reporting. Exportable data in CSV, XLSX, or JSON for regulatory oversight and accountability.

Additional Compliance Coverage

Vendor Certification & Procurement Standards — EO §1

Island's governed MCP Gateway with 500+ integrations ensures third-party AI tools operate within policy. Full auditability supports the new vendor certification requirements DGS and CDT must develop, covering content safety, bias, and civil rights.

Supply Chain Independence — EO §2

If the state CISO determines a federal supply chain designation is improper, agencies need a platform that enforces California-specific procurement rules. Island's policy engine lets agencies define their own approved vendor lists independent of federal designations.

AI Content Watermarking Support — EO §5

Island's audit trails capture the provenance of AI-generated content, supporting the EO's directive for CDT to develop watermarking best practices for AI-generated images and video consistent with California Business & Professional Code §§22757.2–3.

Island Chat: A Vetted GenAI Tool for State Employees

Beyond governing external AI tools, Island offers a built-in, enterprise-governed AI assistant. Island Chat delivers generative AI capabilities—answering questions, drafting content, summarizing pages—with all DLP, privacy, and cybersecurity controls built in. It can serve as the vetted GenAI tool required by EO §4(a).

Why Island for

EO N-5-26 Compliance

SOC 2 Type 2 and ISO 27001 Certified.

Already certified to the highest enterprise security standards. Trusted by government agencies worldwide.

Say yes to AI and comply.

EO N-5-26's intent is responsible adoption, not restriction. Island lets agencies embrace GenAI while meeting every requirement.

One platform, not seven.

Replace fragmented point solutions with a single workspace covering AI access, DLP, security, and auditability.

EO N-5-26 Compliance Checklist

EO N-5-26 Requirement	Island Capability	Section
Facilitate employee access to vetted GenAI tools	AI Access Policy, AI Protection Module	§4(a)
Appropriate privacy safeguards	AI DLP Policy, LLM Training Data Protection	§4(a)
Appropriate cybersecurity safeguards	Browser-native security, ZTNA, Extensions Policy	§4(a)
Vendor certifications for content safety, bias, civil rights	AI Protect, Governed MCP Gateway	§1(a–c)
Supply chain procurement independence	Policy engine, custom vendor lists	§2
Transparency & accountability	Audit logs, SIEM integration, custom dashboards	§4(b–c)
AI content watermarking support	Content provenance audit trails	§5
Vetted GenAI tool for general use	Island Chat (enterprise-governed AI assistant)	§4(a)