AI Governance Policy

VERSION	EFFECTIVE DATE	POLICY OWNER
1.0	2026-07-31	Matt Sapio, CISO

APPROVED BY
Matt Sapio

1. Purpose

This policy establishes a governance framework for the secure and responsible use of AI systems, including large language models (LLMs), AI-enabled automation, and third-party AI services used by Eigenomic. It is designed to protect the confidentiality, integrity, and availability of information and support Eigenomic's SOC 2 security objectives.

2. Scope

This policy applies to AI systems, tools, models, APIs, and services developed, acquired, integrated, or used by Eigenomic in connection with its custom automation software for law offices. It applies to all employees, contractors, and third parties involved in AI-related activities within Eigenomic's fully remote, AWS-based environment.

3. Definitions

- AI Systems: Software, models, and tools that employ machine learning, deep learning, and other AI techniques, including large language models (LLMs).
- Third-Party AI API Providers: External vendors that provide AI capabilities through APIs or hosted services, including data processing and inference services.
- AI Data: Data used as input to, generated by, or otherwise processed through AI systems, including training, testing, validation, inference, prompts, and outputs.

4. Governance and Risk Management

- **Risk Identification and Assessment:**
  - Conduct regular risk assessments specific to AI systems, focusing on potential vulnerabilities, data privacy, and model integrity.
  - AI-related risks must be documented and addressed through Eigenomic's risk management processes.
- **Risk Treatment and Monitoring:**
  - Risk mitigation measures must be appropriate to the AI system's use, sensitivity, and potential impact, and may include testing, validation, human review, access restrictions, and monitoring.
  - AI-related security incidents must be handled in accordance with Eigenomic's Incident Response Plan.

5. Secure AI System Development and Deployment

- **Secure Development Practices:**
  - Integrate secure coding practices and threat modeling into the AI development lifecycle.
  - Regularly review and update AI models and algorithms to address emerging threats and vulnerabilities.
- **LLM and AI Model Protection:**
  - Enforce strict access controls and encryption for training data, model parameters, and outputs.
  - Appropriate safeguards must be applied to protect sensitive AI data, model assets, credentials, and intellectual property from unauthorized access or disclosure.

6. Third-Party AI API Providers

- **Due Diligence and Compliance:**
  - Third-party AI providers must be evaluated based on the sensitivity of data involved, the service provided, and the risks presented to Eigenomic and its customers.
  - Include security and data protection clauses in contracts to ensure third-party providers adhere to the organization’s security standards.
- **Data Handling and Monitoring:**

- Ensure that third-party providers have robust mechanisms for encrypting and protecting data in transit and at rest.
- Require timely notification of security incidents or breaches impacting AI data.

7. Data Segregation and Protection

- **Separation of AI Data:**
  - Implement logical and physical controls to segregate AI training, validation, and production data from other client or operational data.
  - Enforce access restrictions to ensure that only authorized personnel have access to AI data, and maintain detailed audit logs for all data interactions.
- **Data Privacy and Compliance:**
  - AI data must be handled in accordance with applicable legal, contractual, privacy, and security requirements.
  - Use anonymization or pseudonymization techniques where appropriate to protect personal data during AI processing.

8. Operational Security and Monitoring

- **Continuous Monitoring:**
  - AI systems must be monitored at a level appropriate to their risk and use, with suspected security issues reported through established incident reporting procedures.
  - Conduct regular audits and vulnerability assessments on AI systems and infrastructure.
- **Change Management:**
  - Apply formal change management processes to all modifications in AI systems and third-party integrations, including impact analysis and rollback procedures.

9. Roles and Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO)	Owns AI security governance, risk oversight, policy maintenance, and security compliance.
Designated AI/System Owner	Oversees security requirements for assigned AI systems, including access, testing, monitoring, and incident escalation.
Privacy/Compliance Role	Addresses applicable privacy, contractual, and compliance requirements for AI data.
Development and Engineering Teams	Adhere to secure coding practices, conduct regular code reviews, and participate in risk assessments.
Third-Party Management Role	Evaluates and monitors third-party AI providers in accordance with Eigenomic's Third-Party Management Policy.
All Employees and Contractors	Report any potential security incidents or vulnerabilities related to AI systems.

10. Training and Awareness

- **Mandatory Training:**
  - Provide specialized training on AI security, including secure development practices, risk management, and data protection techniques.
  - Ensure periodic refresher training to keep teams updated on emerging threats and evolving regulatory requirements.

11. Exceptions

- **Exception Process:**
  - Any deviations from this policy must be documented, justified, and approved by the designated authority.
  - Exception requests must include a risk assessment and a detailed mitigation plan, and will be reviewed periodically.

12. Violations and Enforcement

- **Enforcement Measures:**
  - Violations of this policy may result in disciplinary action, including termination of employment or contracts, and potential legal consequences.
  - All suspected violations will be investigated, and corrective actions will be implemented to enhance future compliance.