SecureAI

Secure Your AI Adoption with Confidence

As organisations integrate AI into their operations, ensuring robust security and governance is essential. Liquid C2 introduces SecureAI, a specialised service built on our Secure360 solution, designed to help businesses adopt AI securely and responsibly. SecureAI aligns with industry-leading best practices and established global frameworks to provide a comprehensive approach to AI security and compliance.

Our Services

Governance, Risk & Compliance Services

Providing expert guidance to establish strong AI governance:

- **AI Acceptable Use Policy Development** – Define clear guidelines for secure AI use.
- **AI-Data Readiness Assessment** – Ensure secure and compliant AI data handling.
- **AI Governance Framework** – Implement controls and define responsibilities for AI security.
- **AI Risk Assessment** – Identify and mitigate AI-related security vulnerabilities.

Cyber Risk Assurance Services

Ensuring AI applications and infrastructure remain secure:

- **Penetration Testing for AI Chatbots (LLMs)** – Identify vulnerabilities in AI models.
- **Penetration Testing for AI-Integrated Applications** – Secure AI-powered web and mobile applications.
- **API Testing for AI Bots** – Strengthen security for AI-exposed APIs.
- **Code Review for AI-Driven Applications** – Detect and remediate security flaws.
- **AI Infrastructure Architecture Review** – Secure AI environments and data storage.
- **AI Policy Review** – Ensure proper policies for AI model security and compliance.

Liquid C2: Your Trusted Partner in AI Security

With SecureAI, we provide a holistic approach to AI security, ensuring compliance, risk mitigation, and governance excellence.
Adopt AI with confidence – SecureAI by Liquid C2 is here to help!

Interested to learn more?

Read Liquid C2's White Paper
Governance By Design: Ensuring Secure AI Adoption.

Why SecureAI?

- **Comprehensive AI Security**: Governance, risk assessment, and assurance services to protect AI implementations.

- **Industry Best Practices**: Frameworks and policies tailored to align AI adoption with compliance requirements

- **Proactive Risk Mitigation**: Identify and address vulnerabilities before they become threats.

- **Expert-Led Assurance**: Penetration testing, code reviews, and policy evaluations for AI applications.