SecureLLMs.org

Secure AI Platform for the Enterprise

Focus on Innovation, Not Infrastructure

SecureLLMs.org provides businesses with private AI infrastructure on demand.

We deploy advanced Large Language Models (LLMs), including offline versions of ChatGPT, Claude, and over 100 frontier models, in a private environment where your data remains isolated from the public internet.

The platform features built-in model customization, secure knowledge bases for enhanced business context, and flexible role-based access controls. The foundation is an architecture engineered for uncompromising security and reliability.

The SecureLLMs Advantage

Why not just use ChatGPT or Gemini? What’s the risk?

The risk isn't theoretical, it's documented. Google DeepMind researchers demonstrated that prompting ChatGPT to repeat words infinitely caused the model to emit training data verbatim, extracting over 10,000 memorized examples including email addresses, phone numbers, and credentials. Samsung banned ChatGPT entirely after employees leaked proprietary semiconductor source code across three separate incidents. And Cyberhaven's analysis of 7 million workers found that 34.8% of data employees input into AI tools is classified as sensitive, triple the rate from two years prior.

The regulatory exposure is equally concrete. Morgan Stanley paid $35 million for failing to protect customer data through a third-party vendor. The SEC's 2025 Examination Priorities explicitly flag AI governance as a focus area.

Consumer-tier AI tools (ChatGPT, Gemini, Claude) train on your conversations by default. Your proprietary research, client communications, and competitive insights become part of models that serve your competitors.

What makes SecureLLMs different?

SecureLLMs keeps your data protected inside your perimeter. Your chats and files never touch the public internet.

The productivity gains? Custom agents that eliminate repetitive workflows, models that learn your documents in real time and contribute to LLM context, built-in prompt engineering that matches your taste and styles, and the full power of 100+ LLMs, all with unbelievable security? Truly just added benefits on top of carefully architected AI infrastructure.

Why SecureLLMs

AI Infrastructure as a Service

SecureLLMs is not a traditional software as a service (SaaS) product. It's an *extension* of your existing private infrastructure.

The Business and Enterprise plans establish encrypted VPN tunnels that connect directly to your network, creating a secure, continuous bridge between your existing infrastructure and your private AI cloud. Each environment is single-tenant, isolated, and hardened. The Professional tier offers HTTPS/TLS encryption and federation for streamlined access while maintaining the same end-to-end data protection standards trusted by fintech, healthcare, etc.

Dual-Channel VPN Security

Built on enterprise-grade IPsec VPN technology, SecureLLMs establishes dual-channel encrypted tunnels for all model communications. For non-technical readers, this is like digging a literal underground tunnel between your network and secureLLMs environment and running a cable through it that no one else can access. Your chat slides "under" the public internet, reaches your private environment, and the actual language model inference computation stays entirely disconnected from the public internet. Every request travels through both network-layer and SSL/TLS encryption, ensuring LLM-inference traffic stays secure.

VPN tunnels are the industry gold standard for network-layer encryption, backed by NIST SP 800-77.

Three Tiers of Private AI Security

Professional Tier – $2,000/month + token usage
Up to 10 users, 3 AI models included, HTTPS/TLS encryption and federated authentication for endpoint control.

Business Tier – $5,000/month + token usage
Up to 50 users, access to all AI models, VPN encryption via fast VPN Client installation on endpoint devices.

Enterprise Tier – $10,000+/month + token usage
*****Unlimited users, access to all AI models, IPSec Tunnel via Site to Site VPN, accesses models via private link, and integrates directly with Oauth, OIDC, and Okta identity providers.

*Enterprise Tier: $100 per user, per month over 100 users.

All tiers include an installation fee equivalent to one month of tier.

The Future of Private AI

SecureLLMs bridges the gap between cutting-edge AI and enterprise-grade security, delivering intelligence at the speed of innovation, protected by infrastructure you can trust.

Website: https://securellms.org
Schedule a Demo/Contact: michael@securellms.org

In a world where intelligence is abundant, private data is the only competitive edge we have left.