Geniuspace ® — 政府/企业简报

AI 创新算法/方法：治理、安全、审计证据链与可控部署。

1) 定位

- 面向政府部门、关键基础设施与大型企业：以 “ 证据 ” 驱动决策。
- 把战略目标转化为可审计的 AI 运行体系（流程 + 交付物）。
- 部署形态：本地/专有云(VPC)/隔离环境/边缘（小模型 SLM）。

2) 可招采交付物

- 架构方案：目标技术栈、模型策略、RAG、可观测性。
- 治理章程：RACI、政策、评审节奏、紧急停止、事件响应。
- 评测套件：测试集、指标、报告、上线/下线门禁。
- 招采材料包：需求、SLA、安全与可逆性条款。

3) 信任与合规要求

- 审计证据链：日志、版本、审批、数据血缘与决策记录。
- 安全：RBAC、加密、隔离、DLP、防外泄、红队测试。
- 合规：基于风险的流程 + 证据（需结合 PIPL/DSL/CSL 等具体范围）。

说明：本简报用于构建审计材料；请结合行业与地区法规获取法律意见。