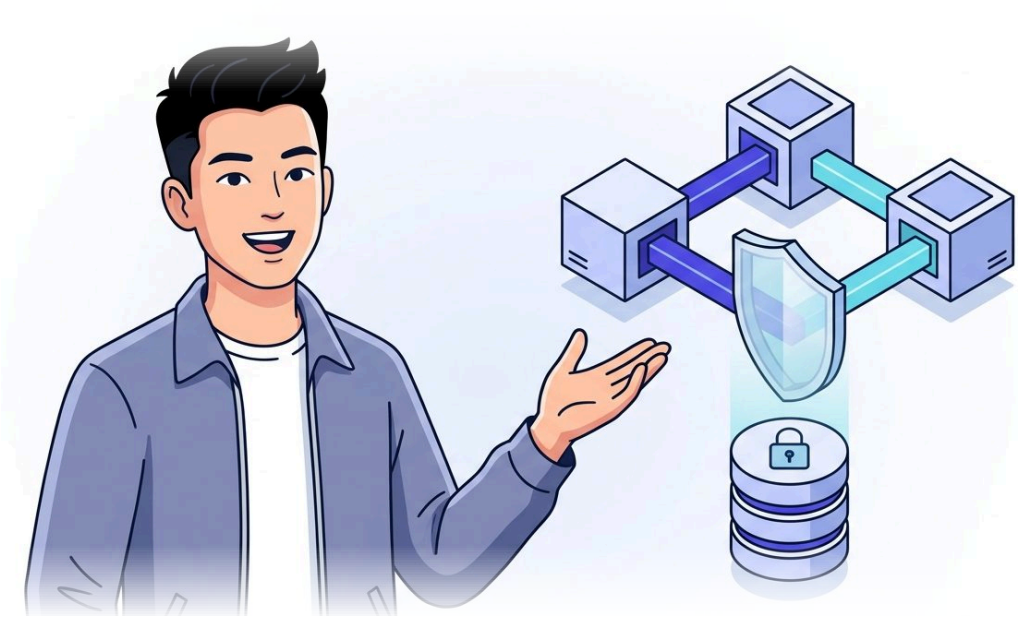
安全与内控红线

五条架构级设计约束、客户自查核验方法与可直接纳入交付协议的合同技术附件签署页。



05
条架构级硬性安全红线

00
个业务数据库直连写账号

01
页可直接入合同的签署附件

发布机构
诺石数智

版本日期
v1.0 · 2026-11

适用角色
法务 / 财务 / 内审 / 信息部

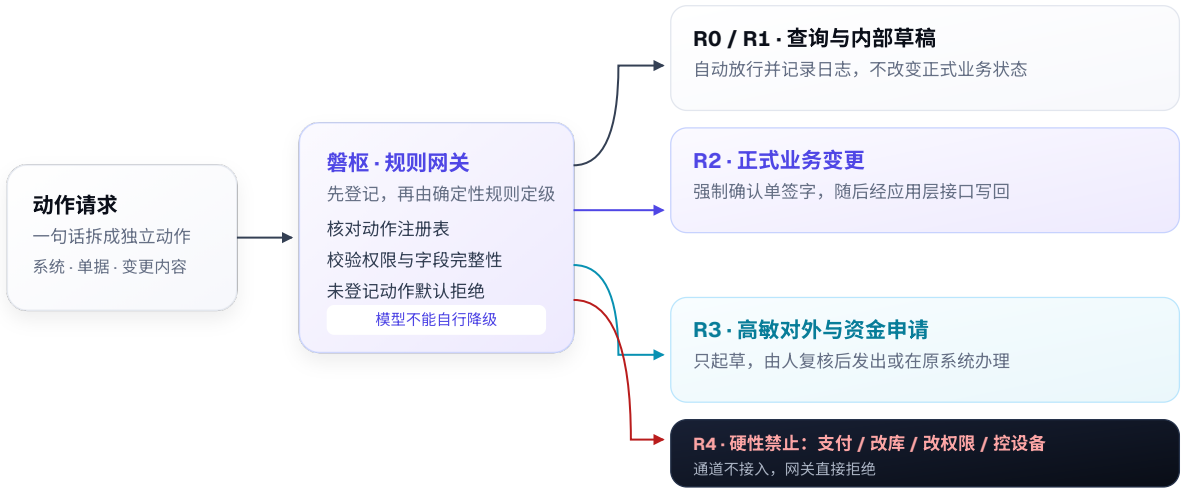
官方网站
www.nerss.com

设计约束声明与网关拦截位置

> 本文件所列五条安全与内控红线，不是事后统计的成功率，而是**系统在架构设计上就不提供越界路径**。无论对话内容如何诱导，越界请求均在应用与网关层被确定性拦截。

本文件面向企业法务、财务负责人、内审与信息安全团队，用于项目立项审查、安全评审以及作为正式交付合同的技术附件。所有条款均配套客户方可独立执行的核验步骤。

图 1 · 磐枢规则网关拦截位置与五条红线执行边界　　规则代码硬判定 · 未登记动作一律默认拒绝



五级风险分级与红线对应总表

级别	典型业务动作	网关硬性放行方式	对应红线
R0	只读查询订单、库存与生效制度	**按岗位权限自动放行并记录日志**	红线 02（仅应用层只读）
R1	内部草稿、报销与合同异常标注	**不改变正式业务状态，供人工终审**	红线 03（不替代人工审批）
R2	交期变更、售后补发、现场派工	**强制生成确认单，授权主管签字后写回**	红线 02 + 红线 03
R3	付款/退款申请、对外客户函、合同签发	**AI 仅起草草稿，由人工核对后发出或办理**	红线 01 + 红线 03
R4	打款支付、直改/删库、改权限、控设备	**通道不接入，网关层硬性禁止拒绝**	红线 01 / 02 / 04

安全与内控红线（01 至 03 条）

围绕资金执行隔离、存量业务库保护与正式变更签字权三大高频内控关切，明确技术拦截层与独立核验法。

红线 01 · 资金只起草，支付不接入

架构硬约束

红线条款原文

资金申请只起草（R3），支付执行不接入（R4）。

业务语言含义

涉及付款、划转、退款的申请仅生成凭证与草稿，由财务人员在原有资金系统内审核办理；智能体不具备打款、转账与支付接口调用能力。

系统拦截层级

磐枢规则网关（R4 禁入白名单）与接口连接器层物理隔离，不注册任何支付类动作与网银凭证。

客户方自查核验方法

信息部与财务可核查已注册动作清单及连接器凭据，确认无任何资金划转、银行直连或支付接口接入。

红线 02 · 不直接读写业务数据库

架构硬约束

红线条款原文

任何接入级别均不直接读写存量业务数据库。

业务语言含义

不绕过原有 ERP、OA、CRM、WMS 的业务校验、权限与事务审计，不破坏原厂维保条款，杜绝脏写与账实不符。

系统拦截层级

严格按 L1 官方接口 → L2 原审批流 → L3 只读同步 → L4 有限界面自动化顺序经应用层交互。

客户方自查核验方法

客户 DBA 核对分配给诺石平台的全部账号清单，确认未授予任何业务数据库直连读写权限。

红线 03 · 正式变更必须签字放行

架构硬约束

红线条款原文

R0–R1 自动放行；R2 正式变更须授权人签字放行；R3 对外发送与合同签发仅起草。

业务语言含义

智能体承担查单、核对与备单工作，所有改变正式业务状态的动作均须经岗位授权人在确认单上核对原文并签字后才写回系统。

系统拦截层级

磐枢规则网关强制拦截未签名 R2 动作；确认单须具备唯一签字记录与时间戳方可触发下游接口。

客户方自查核验方法

审计团队可随机抽取任意已写回业务单号，在审计账本中核对对应的确认单编号、签字人及制度版本号。

安全与内控红线（04 至 05 条）与不做清单

红线 04 · 不直控设备，不改权限

架构硬约束

红线条款原文

不下发生产设备控制指令，不修改账号、角色与系统权限配置（R4 禁止）。

业务语言含义

工单协同仅到派工与排障建议层面，绝不碰 PLC/SCADA 工业控制；组织架构与权限变更严格保留给企业 IT 管理员。

系统拦截层级

网关动作注册表硬性封禁工控协议与身份权限管理接口（IAM/RBAC 写操作）。

客户方自查核验方法

信息安全负责人检查网络访问控制策略与动作注册表，确认无工业控制网段连通及权限写入接口。

红线 05 · 客户数据绝不用于训练

架构硬约束

红线条款原文

客户业务数据、历史单据、价格条款与知识资产绝不用于公共大模型训练。

业务语言含义

企业的核心报价口径、客户名录、合同条款与老师傅排障经验始终属于企业自有资产，不外泄、不反哺通用模型。

系统拦截层级

企业数据仅存储于客户指定环境（专属云或私有化机房），模型调用采用零留存协议并支持本地私有模型部署。

客户方自查核验方法

法务与安全团队可审阅合同数据主权附件、网关出口日志及部署网络拓扑，核验数据驻留范围。

诺石数智明确不做的四件事

不做脱离制度的通用聊天助手

不以通用写周报、泛化聊天为交付目标，聚焦接进现有业务系统的受控执行与有据接待。

不让 AI 触碰资金执行、删数据与改权限

打款支付、批量删除业务记录、修改用户权限与直控生产设备一律列为 R4 网关硬禁止。

不直接读写存量系统业务数据库

绝不索要 ERP/OA 底层数据库读写账号，确保原厂维保、业务事务与审计链完整无损。

不作虚浮承诺与拉踩对比

不承诺「替代人工」「零差错」「保证搜索排名第几」或空泛的「节省人力百分比」，也不点名贬低竞品。

责任边界与偏离处置：在交付测试或影子运行期间，如客户核验发现任一接口或动作配置偏离上述五条红线，客户有权要求立即暂停测试与写入并由诺石在整改复测通过后方可继续推进。

附页：交付合同安全与内控红线技术附件（参考签署页）

本页可独立打印，经甲乙双方确认勾选后作为主交付合同之技术附件生效，与主合同具有同等约束力。

交付合同安全与内控红线技术附件

NERSS-SEC-01 · 附件编号：_____

兹就甲方（客户单位）与乙方（诺石数智（杭州）网络科技有限公司）所签企业智能运营项目主合同，双方明确约定以下五项架构级安全与内控约束：

勾选	约束项	合同硬性约束内容	甲方验收核验方式
☐ 确认	**01 资金支付隔离**	付款与退款申请仅出草稿（R3），不接入任何打款与支付通道（R4）。	核查动作清单与连接器凭据
☐ 确认	**02 禁止直改业务库**	仅经 L1–L4 应用层接入，乙方不申请且不持有业务数据库读写账号。	甲方 DBA 核查全部账号权限
☐ 确认	**03 正式变更须签字**	R2 正式变更必经确认单签字后写回；R3 对外发出由人工复核执行。	抽查审计账本与确认单签字
☐ 确认	**04 不控设备不改权**	不下发工业生产设备控制指令，不修改员工账户、角色与系统权限。	检查网段隔离与网关禁用表
☐ 确认	**05 数据不用于训练**	甲方业务单据、价格与知识资产归甲方所有，绝不用于公共模型训练。	核验部署环境与零留存协议

补充约定：本项目选择部署形态为：☐ 公有云（仅对外公开资料） ☐ 专属云隔离实例 ☐ 甲方自有机房本地私有化。
项目上线前，乙方须配合甲方完成脱敏真单据评测与一键停用 AI 应急演练，确认 R2–R4 高风险动作漏拦数为 0 后方可开放正式写回。

甲方（盖章）：_____

授权代表签字：_____

信息安全 / 法务复核：_____

签署日期：_____ 年 ____ 月 ____ 日

乙方（诺石数智（杭州）网络科技有限公司盖章）：

_____

授权代表签字：_____

项目架构负责人：_____

签署日期：_____ 年 ____ 月 ____ 日

配套公开文件体系（www.nerss.com/compliance/）

可与《企业级智能体开发规约 v0.1》《NERSS 实验室评测方法》《数字资产主权与部署规范》配合使用。

诺石数智：www.nerss.com
工作日 4 小时内响应