等保 2.0 三级 符合性自评报告
v0.1-draft
draft
sha256:a7c5d4e3f…
⊙ draft · CONFIDENTIAL
Argus Gateway
Argus Gateway · v0.1-draft
GB/T 22239-2019

等保 2.0 三级 符合性自评报告

Argus Gateway 产品级 GB/T 22239-2019 三级技术要求 符合性自评说明 · 草案待 review

客户
Argus Gateway 产品
审计周期
2026-01-01 ~ 2026-06-30
生效日期
2026-07-15
文档版本
v0.1-draft
网关版本
v1.6.0 · 9 adapters · 56 PII types

agilist.cn · Argus Gateway
sha256:a7c5d4e3f2a1b0c9d8e7f6a5b4c3d2e1f0a9b8c7d6e5f4a3b2c1d0e9f8a7b6c5

目录

GB/T 22239-2019 条款对照

条款	Argus Gateway 实现	证据指针	客户责任边界
8.1.2.1 网络架构	Argus Gateway 部署于客户 DMZ；客户内网 → Gateway → 上游	https://argus.agilist.cn/docs/	客户网络拓扑图 / VLAN 分区 / DMZ

条款	Argus Gateway 实现	证据指针	客户责任边界
	LLM 全链路 TLS 1.2+。Gateway 自身不提供网络分区设计。	architecture/network-topology	ACL 由客户整体系统设计
8.1.2.2 通信传输	上游 LLM 链路统一 HTTPS (TLS 1.2+) + hostname verify + CA pinning。Admin 后台默认 HTTPS。配置态 API Key / 上游 credentials 走 vault 加密落库。	https://argus.agilist.cn/docs/security/tls-config	客户证书签发 + 私钥保管 + 内网 → Gateway 段 TLS 由客户决定
8.1.3.1 边界防护	Argus Gateway 拒绝未知 content-type, 仅 application/json + text/event-stream; 请求体超 size 上限即拒。	https://argus.agilist.cn/docs/security/content-filter	客户入站 WAF / 反向代理边界由客户系统承担
8.1.3.2 访问控制	请求侧多租户 API Key + 路由策略 + Workspace 隔离；后台 LDAP/SAML/OIDC 三选一 SSO 接入。	https://argus.agilist.cn/docs/admin/access-control	客户内部角色分配 + Key 季度轮换 + 离职及时回收
8.1.3.3 入侵防范	rate-limit 多维（per-IP / per-tenant / per-endpoint) + 异常 PII 暴增模式触发自动告警 + 拒绝异常流量。	https://argus.agilist.cn/docs/admin/rate-limit	告警渠道（邮件/钉钉/企微/PagerDuty) 由客户接入 + 阈值客户调
8.1.4.1 身份鉴别	API Key 多租户 + LDAP/SAML/OIDC 三选一 SSO 接入后台；Key rotation 强制季度。	https://argus.agilist.cn/docs/auth/sso	客户 IdP 配置 + 账号生命周期管理
8.1.4.2 访问控制	RBAC 三角色（viewer/operator/admin); 审计日志只读，后台不可删改。Workspace 隔离防 cross-tenant 数据泄漏。	https://argus.agilist.cn/docs/admin/rbac	客户内部角色分配 + 离职回收
8.1.4.3 安全审计	每个代理请求落审计（request_id / tenant / user / pii_count / ts / upstream_status / 路由决策)，append-only SQLite + 日切归档。	https://argus.agilist.cn/docs/admin/audit-log	审计日志保留 ≥ 6 个月 + 离线备份（网安法 §21 要求）
8.1.4.4 入侵防范	请求体异常（超 size / 异常 PII 模式）触发自动告警 + 拒绝；上游 LLM 连接重置自动 fail-over。	https://argus.agilist.cn/docs/admin/alerts	客户应用端 input sanitize + Gateway 告警渠道接入
8.1.4.5 恶意代码防范	请求/响应 payload 仅允许 application/json + text/event-stream; 二进制 / multipart upload 默认拒。	https://argus.agilist.cn/docs/security/content-filter	客户应用端反病毒由客户系统承担
8.1.4.7 数据完整性	审计日志 HMAC-SHA256 链式签名，任何篡改在下次校验时检出；配置变更走 git-backed audit。	https://argus.agilist.cn/docs/admin/integrity-chain	HMAC 密钥客户托管（不存 Argus Gateway) + 配置 git remote 客户备份
8.1.4.8 数据保密性	PII 脱敏后才入上游 LLM (56 类 L1 正则 + 可选 L2 NER); response 还原仅在客户侧 token map 持有期间；配置态 vault 加密。	https://argus.agilist.cn/docs/security/pii-redact	Token map TTL 客户配置 + 客户侧 LLM 上下文管理
	SQLite 落地 + 日切 + S3-compatible offsite (可选)。RPO 24h,		

条款	Argus Gateway 实现	证据指针	客户责任边界
8.1.4.9 数据备份恢复	RTO ≤ 4h (单实例); HA 集群 RTO ≤ 5min。	https://argus.agilist.cn/docs/ops/backup	S3 桶 + 灾备地点客户提供 + RTO 演练客户排程
8.1.4.10 剩余信息保护	请求结束后 token map TTL 到期自动 purge, 内存 wipe 不写盘；审计日志归档后原文件加密删除。	https://argus.agilist.cn/docs/security/token-lifecycle	TTL 配置审计 + 客户侧 token map 一致清理
8.1.4.11 个人信息保护	PIPL §13/55 — 处理目的限定为 LLM 转发；默认不长留；DPIA 报告模板独立成卷（Admin UI DPIA Panel)。	https://argus.agilist.cn/docs/compliance/pipl	客户知情同意 + DPO 联络人 + DPIA 实际评估
8.1.5.1 系统管理	Admin UI 三角色 + 操作审计（系统配置变更 / 角色变更 / 密钥轮换 全留痕)。	https://argus.agilist.cn/docs/admin/system-admin	客户内部系统管理员岗位 + 操作 SOP 由客户制定
8.1.5.2 审计管理	审计日志独立角色（auditor 只读）+ 审计动作不可被 admin 静默删除；审计自审 log。	https://argus.agilist.cn/docs/admin/auditor-role	客户审计员岗位 + 审计自查制度
8.1.5.3 安全管理	Workspace 边界 + 多租户隔离 + 策略集中下发；Gateway 自身策略 git 化，peer review 配置变更。	https://argus.agilist.cn/docs/admin/policy-management	客户整体安全管理制度 + 安全管理员岗位由客户系统承担
8.1.5.4 集中管控	Admin Dashboard 多 Workspace 统一视图 + Prometheus / Grafana metrics 集中。	https://argus.agilist.cn/docs/admin/dashboard	客户集中安全管理中心（SOC）由客户系统设计 + Gateway 仅提供 metrics 喂入

证据指针

E

审计日志 API 规范 · https://argus.agilist.cn/docs/admin/audit-log

E

PII 脱敏统计仪表盘 · https://argus.agilist.cn/docs/admin/redact-stats

E
RBAC 角色矩阵 · https://argus.agilist.cn/docs/admin/rbac

E
网关部署 + 网络拓扑 · https://argus.agilist.cn/docs/architecture/network-topology

E
Argus Gateway 公开文档首页 · https://argus.agilist.cn/docs

免责声明

本报告系 Argus Gateway 就 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》三级安全要求所开展的**产品级符合性自评说明**，不属于、也不替代由具备资质的等级保护测评机构依法开展的等级测评，亦不构成任何形式的等级保护认证或“已通过等保”的结论。

网络安全等级保护的定级、备案与等级测评，依法由信息系统的运营、使用单位（即客户作为网络运营者）承担（“谁运营谁负责”原则）。本报告仅就 Argus Gateway 作为客户信息系统组成部分时，可为相关控制项提供的技术支撑进行说明，供客户及其委托的测评机构对照参考。客户系统能否满足等保三级要求，取决于客户的整体系统设计、配套管理措施与实际运营。

本报告不构成法律意见，亦不替代企业自有的合规 / 法务团队判断。本报告所述结论以编制日产品状态为准。

签章

本页提供盖章位与签字栏，请在打印件上手签 + 加盖公章。盖章位为 82×82mm 国标公章尺寸。

请加盖公章
82 × 82 mm
Argus Gateway 产品
签发人
2026-07-15
签发日期

客户签字

客户日期