# 等保 2.0 三级 对照白皮书

Argus Gateway · 企业 AI 隐私网关 · 产品级符合性自评说明 · 示意版 v0.1 · 更新于 2026-05-23 · 爱科拓 (agilist.cn)

本白皮书示意 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》三级安全要求与 Argus Gateway 作为客户信息系统组件时可提供的技术支撑方向。 本文件为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，不构成任何形式的等级保护认证结论。

> 阅读说明： 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。 本文件仅就 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。 详细映射、evidence 字段、配套技术说明，请在申请 demo 后由 Argus Gateway 团队随部署方案一起提供。

## 1. Argus Gateway 在等保 2.0 三级合规链路中的定位

等保 2.0（GB/T 22239-2019）的定级、备案与测评对象是客户的信息系统，而不是单一软件产品。 "通过等保"作为针对客户系统的等级测评结论，依法只能由具备资质的等级保护测评机构出具，Argus Gateway 自身不构成任何"已通过等保"的产品声明。

Argus Gateway 处于企业内部用户与上游 LLM 服务之间，作为客户三级信息系统的一类技术组件，可在多项三级要求上提供数据平面支撑：

- 身份与访问层：API Key 鉴权 + 部门 / 角色级 RBAC + 路由策略，对应 8.1.4.1 身份鉴别 / 8.1.4.2 访问控制。
- 审计层：结构化审计日志（身份 / 时间 / 脱敏命中 / 路由决策 / 上游后端 / 成本归因），对应 8.1.4.3 安全审计 / 8.1.5.2 审计管理。
- 数据层：L1 正则 + L1b 证据评分 + L2 开放词汇 PII 脱敏，对应 8.1.4.7 数据完整性 / 8.1.4.8 数据保密性 / 8.1.4.11 个人信息保护。
- 通信层：对上游 LLM 的 HTTPS 传输 + 配置态保密，对应 8.1.3.2 通信传输。

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。本表所列均为 Argus Gateway 可作为组件之一提供的方向性支撑，不构成对客户系统整体合规性的判断。

## 2. GB/T 22239-2019 三级 控制项 × Argus Gateway 能力方向

下表按 GB/T 22239-2019 三级"安全通信网络 / 安全计算环境 / 安全管理中心"三类，列出 Argus Gateway 有直接数据平面贡献的 11 项控制项。 其余条款（物理安全 / 网络架构 / 系统管理流程 / 安全管理制度等）由客户整体系统设计与运营覆盖，不在本文件范围。

| 控制项编号 | 要求描述 | Argus Gateway 能力方向 | evidence 字段 |
| --- | --- | --- | --- |
| 8.1.3.2 通信传输 | 应采用密码技术保证通信过程中数据的完整性与保密性。 | Argus Gateway 与上游 LLM 之间的请求/响应链路统一走 HTTPS（TLS 1.2+）；管理后台默认 HTTPS；上游凭证 / API Key 在配置态加密落库（vault）。 | test_br_https_only_upstream / vault 加密栈 / nginx vhost TLS 配置 |
| 8.1.4.1 身份鉴别 | 应对登录的用户进行身份标识与鉴别，标识具有唯一性，鉴别 | 客户端 API Key（唯一、可吊销、可轮换）+ 管理后台账号 bcrypt 密码 + TOTP 二次验证（双因素鉴别）+ 路由级鉴权；失败计数 + 锁定阈值可配置。 | test_br_invalid_key_returns_401 / test_br_admin_login_lockout / test_br_password_policy / test_br_alembic_totp_migration / api_keys 表 |

| 控制项编号 | 要求描述 | Argus Gateway 能力方向 | evidence 字段 |
| --- | --- | --- | --- |
| | 信息具有复杂度并定期更换。 | | |
| 8.1.4.2 访问控制 | 应依据安全策略控制用户对资源的访问，授权主体配置访问规则，规则覆盖主体与客体之间的操作。 | 部门 / 角色级 RBAC + 上游路由策略 + key→部门→上游 多层约束；越权请求由 proxy 端在脱敏前拒绝。 | test_br_rbac_enforcement / test_br_upstream_routing_policy / audit_log.deny 维度 |
| 8.1.4.3 安全审计 | 应启用安全审 | 每次代理请求生成结构化审计记录，包含 | |

| 控制项编号 | 要求描述 | Argus Gateway 能力方向 | evidence 字段 |
| --- | --- | --- | --- |
| | 计功能，审计覆盖每个用户，对重要的用户行为和重要安全事件进行审计。 | 请求方身份 / 路由决策 / 脱敏命中 / 上游后端 / 响应时长 / 成本归因；管理后台与导出 API 可按维度切片。 | test_br_audit_log_written / audit_log schema / docs/user-guide/audit-compliance.md |
| 8.1.4.4 入侵防范 | 应能够发现可能存在的已知漏洞并及时修补；应限制非法连接，关闭不需要的 | Argus Gateway 仅对外暴露 proxy / admin 两类端口；依赖版本由 CI 锁定（pip-tools 锁文件）；不必要服务（默认账号、guest 上传等）默认关闭，发布前由 invariant 测试自动巡检。 | test_invariant_no_default_admin_password / test_invariant_no_open_signup / requirements.lock |

| 控制项编号 | 要求描述 | Argus Gateway 能力方向 | evidence 字段 |
| --- | --- | --- | --- |
| | 系统服务、默认共享和高危端口。 | | |
| 8.1.4.10 剩余信息保护 | 应保证鉴别信息所在的存储空间，被释放或重新分配前得到完全清除。 | 脱敏映射表 (key) 默认仅驻内存、不落盘；admin session token 退出/超时即销毁；密钥/凭证清退走 vault 删除接口。 | test_br_redact_key_in_memory_only / test_br_admin_session_invalidation |
| 8.1.4.7 数据完整性 | 应采用校验技术或密码技术保证重要数据 | 审计日志按行追加只写、链上不允许就地改写（append-only 语义）；配置变更 / RBAC 调整有变更记录；上 | test_br_audit_log_append_only / test_br_restore_mapping_consistency |

| 控制项编号 | 要求描述 | Argus Gateway 能力方向 | evidence 字段 |
| --- | --- | --- | --- |
| | 在传输和存储过程中的完整性。 | 游响应还原阶段对脱敏 key→明文 映射做一致性校验，映射不一致直接拒绝输出。 | |
| 8.1.4.8 数据保密性 | 应采用密码技术保证重要数据在传输和存储过程中的保密性。 | 上游 API Key / SMTP 密码 / Webhook 签名密钥等敏感配置在 vault 加密落库；管理后台不回显明文密钥；审计日志中 PII 默认以脱敏占位符形式呈现。 | vault Fernet 加密栈 / test_br_admin_key_not_echoed / audit_log redact_placeholder |
| 8.1.4.11 个人信息保护 | 应仅采集和保存业务必需的用户个人信息；应禁止未 | 多层 PII 识别与脱敏在请求进入上游前完成；脱敏映射本地保留、不外发；管理后台对 PII 详情的访问受 RBAC 控制，越权访问由 | test_br_pii_never_in_upstream / argus-redact L1+L1b+L2 / docs/user-guide/audit-compliance.md |

| 控制项编号 | 要求描述 | Argus Gateway 能力方向 | evidence 字段 |
| --- | --- | --- | --- |
| | 授权访问和非法使用用户个人信息。 | audit_log 留痕。 | |
| 8.1.5.2 审计管理 | 应对审计记录进行集中管理，按需求对审计记录进行分类、汇总、统计、查询和分析。 | 审计日志统一落入审计存储；管理后台提供按部门 / 用户 / 上游 / 时间 / 脱敏类型 维度的聚合视图与导出；可对接客户 SIEM。 | audit_log 索引设计 / 管理后台 audit 页 / docs/user-guide/audit-compliance.md |
| 8.1.5.4 集中管控 | 应建立集中的安全 | 管理后台对 keys / 上游路由 / RBAC / 审 | 管理后台模块结构 / 配置变更 audit / docs/user-guide/admin-overview.md |

| 控制项编号 | 要求描述 | Argus Gateway 能力方向 | evidence 字段 |
| --- | --- | --- | --- |
| | 管理中心，对分布在不同区域的安全设备或安全组件进行管理。 | 计 / 成本归因等模块提供集中入口；配置变更、上游切换、key 吊销均通过单一控制面下发并留存审计。 | |

## 3. 几个核心控制项的展开说明

### 3.1 8.1.4.3 安全审计 与 8.1.5.2 审计管理

Argus Gateway 为每次代理请求生成结构化审计记录，字段覆盖请求方身份（API Key / 部门 / 员工）、时间、脱敏层命中情况与 PII 类型分布、路由决策与上游后端、响应时长与成本归因。 审计记录在写入时采用追加只写语义（同 8.1.4.7 数据完整性），并提供按维度的聚合视图与导出接口，方便客户集中归集到统一审计平台（SIEM）。 日志保留期可配置，建议与等保三级、PIPL 第十九条 "合理期限" 协调，并预留事后回溯所需时长。

### 3.2 8.1.4.11 个人信息保护 与 数据脱敏

Argus Gateway 在请求进入上游 LLM 服务前进行多层 PII 识别与脱敏，覆盖中国常见结构化 PII（身份证 / 银行卡 / 手机 / 邮箱 / 地址 / 港澳台身份证 / 企业统一社会信用代码等），并对中文姓名 / 组织名 / 地名等开放词汇 PII 类型作扩展支持。 脱敏后的请求转发到上游 LLM，原始 PII 仅在 Argus Gateway 本地保留映射，响应阶段做还原。核心算法（argus-redact）已开源，企业可独立验证识别效果。

### 3.3 不在本表范围的等保三级要求

物理与环境安全（8.1.1 物理位置选择 / 物理访问控制 / 防盗窃和防破坏等）、网络架构（8.1.3.1 / 8.1.3.3）、安全管理制度与人员管理（8.2 系列）、应急响应与运维管理等条款，由客户机房 / 网络 / 流程整体覆盖，不构成 Argus Gateway 产品级支撑范围。客户在等保测评时应将本表作为组件级支撑材料嵌入整体系统说明。

## 4. 使用建议

- 客户在开展等保三级备案 / 测评前，应由本单位网络安全负责人完成定级、备案手续，并将 Argus Gateway 列为信息系统组成中的一类技术组件。
- 测评机构在对照 GB/T 22239-2019 三级要求时，可参考本文件第 2 节四列表，按"控制项编号 → Argus Gateway 能力方向 → evidence 字段"链路索取具体技术证据。
- Argus Gateway 提供的技术说明材料、配置模板均为支撑性参考，最终等保测评结论以测评机构出具版本为准。
- 审计日志保留期、密码套件版本、上游路由策略等参数由客户在选型评估阶段与 Argus Gateway 团队联合确认。

免责声明： 本文件系 Argus Gateway 就 GB/T 22239-2019 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。本文件仅就 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。 本文件不构成法律意见，亦不替代企业自有的合规 / 法务团队判断。本文件所述结论以编制日产品状态为准。