

Oneasy 客户侧智能体服务治理与使用规范

——《Oneasy SaaS 服务协议》之智能体服务专项附录

项目	内容
文件编号	OY-GOV-AI-001
版本	V1.1
文件性质	《Oneasy SaaS 服务协议》之智能体服务专项附录
状态	优化稿（待 GloryScience 正式批准与发布）
发布主体	GloryScience International Limited（以下简称“GloryScience”）
产品品牌	Oneasy
最后更新日期	2026年7月27日
生效日期	以本规范第11条约定为准
适用语言	简体中文；如另行发布其他语言版本，由订单或正式发布文件指定控制语言；未指定的，以简体中文版本为准
复审周期	至少每十二（12）个月一次，或在服务、适用法律、数据处理方式、第三方模型、功能边界或风险状况发生实质变化时复审

重要提示

- Oneasy 智能体能力用于辅助知识检索、信息理解、分析、诊断、草拟和流程协作，不替代具备相应权限和能力的工程师、安全人员、管理人员或用户的最终判断。
- 智能体输出可能存在不完整、不准确、过时、误判、遗漏、上下文缺失或设备适配差异。涉及生产网络、高风险网络操作、监管、合同、安全事件或对外发布时，必须完成适当的人工复核和内部审批。
- 智能体对话、自然语言指令、参数预填、一般性确认或建议采纳，不当然构成对外部执行或生产网络变更的有效授权。
- 用户始终保留对其网络、设备、数据、业务流程、授权用户及生产变更的最终控制。本条不排除或限制 GloryScience 根据主协议、适用 DPA、Security Addendum、其他书面文件或强制性法律应承担的义务。

1. 目的、适用范围与文件关系

1.1 目的与法律性质

本《Oneasy 客户侧智能体服务治理与使用规范》（以下简称“本规范”）规定用户及其授权用户在使用 Oneasy 智能体能力时的数据、权限、人工复核、外部执行、生产网络控制、禁止用途及事件协作

规则。

本规范是《Oneasy SaaS 服务协议》（以下简称“主协议”）的智能体服务专项附录。在本规范通过订单、订阅页面、管理后台、产品内勾选、功能启用流程或其他可记录方式被明确引用，并由用户或其授权代表有效接受后，本规范构成主协议不可分割的组成部分。

本规范未定义的术语，具有主协议赋予的相同含义。

1.2 适用对象与能力范围

本规范适用于：

- 已开通、启用、访问或实际使用 Oneasy 智能体能力的用户；
- 用户的租户管理员和授权用户；
- 经用户合法授权，在用户租户内使用智能体能力的系统集成商、托管运维团队、顾问、承包商或其他第三方。

本规范仅适用于已经正式发布、包含于用户订阅或试用范围、并在用户租户中实际启用的智能体能力。AI Assistant、OnExpert、OnTwin、Oneasy 智能运维智能体或其他名称，仅在对应能力符合前述条件时适用。

智能体名称、品牌架构、演示、营销材料、路线图、概念说明或本规范中的治理分类，不构成未发布、未订购、未启用功能的交付、性能、兼容性、准确性、服务结果或持续可用性承诺。

1.3 与其他文件的关系

本规范就智能体能力的用户输入、人工复核、数据与权限管理、外部执行、高风险网络操作、禁止用途及智能体相关事件协作等专项事项，对主协议进行补充。

不同文件同时适用时：

1. 订单、Subscription Order、SOW、Enterprise SLA 或经授权签署的专项书面协议，仅就其明确约定的订阅、价格、期限、部署、实施、支持、服务等级或其他专项事项优先；
2. 涉及个人数据处理、跨境传输、子处理者、数据主体请求或数据保护法定义务的，以适用 DPA 及强制性法律要求为准；
3. 涉及安全控制、远程接入、安全事件响应或其他专项安全事项的，以适用的 Security Addendum 为准；
4. 涉及费用、支付、退款、知识产权、一般责任限制、赔偿、终止、法律适用及争议解决等事项的，以主协议及其他对应专项文件为准；
5. 本规范不得被解释为扩大 GloryScience 在主协议、订单、DPA、Security Addendum 或 SLA 项下未明确承担的服务义务、功能承诺、服务等级或责任范围。

1.4 用户对授权人员和第三方的管理

用户应确保其租户管理员、授权用户及经授权第三方在使用智能体能力前知悉并遵守本规范。用户应通过合同、内部制度、权限配置或其他合理方式，使经其授权使用用户租户的第三方承担不低于

本规范的保密、安全、权限、数据和高风险操作义务。

系统集成商、托管运维团队或其他代表多个最终客户使用 Oneasy 的主体，应确保其已经取得相应网络所有人、运营方或数据责任主体的有效授权，并对不同客户、租户、账号、数据、凭据和操作实施合理隔离。

2. 术语

术语	含义
智能体能力	Oneasy 通过人工智能模型、机器学习、RAG、知识库、工具调用、受控接口、工作流或其他类似技术提供的问答、检索、分析、可视化、建议、草拟、诊断辅助、任务编排或其他已正式发布并启用的 AI 辅助功能。
智能体输出	智能体能力自动或半自动生成的文本、代码、分析、配置建议、诊断思路、根因推断、任务建议、图表、摘要、参数预填或其他 AIGC。
用户输入	用户或授权用户向智能体能力输入、上传、连接、授权调用或指示处理的用户内容、客户网络数据、电信运维数据、第三方技术资料、提示词、文件、日志、配置、命令、截图、接口数据或其他信息。
外部执行	可能改变用户或第三方系统、数据、设备、权限、公开内容、业务流程或运行状态的操作，包括通过接口、工具、脚本、工作流、自动化或远程接入触发的操作。
高风险网络操作	可能影响生产网络、终端用户服务、业务连续性、网络安全、数据完整性或监管合规的配置、命令、脚本、自动化、远程接入或其他操作。
运维核验依据	用于核对特定设备、网络、任务或事件的现场数据、经批准的变更记录、设备实际返回结果、正式设备厂商资料、适用法律、合同文件或经授权确认的其他记录。
网络接入组件	用于设备连接、云边接入或远程运维的 Oneasy Agent、Connector、VPN、API Token 或类似技术组件。网络接入组件不因使用“Agent”名称而当然属于本规范所称的智能体能力。

3. 角色与责任

主体	主要责任
用户	对其业务目的、数据合法性、网络和设备授权、生产变更、内部审批、业务连续性及授权人员管理承担相应责任；确保已取得使用智能体和接入相关系统所需的合法授权。
租户管理员	管理用户、角色、智能体功能、知识库、数据接入、第三方连接和凭据；建立人工复核、变更、外部执行及事件处置流程；定期回收不再需要的权限和连接。
授权用户	仅在获授权限和工作需要范围内使用智能体；核验关键输出；不得绕过审批、访问控制、数据边界或生产网络控制。
经授权第三方	仅在用户授权范围内使用相应租户和数据；不得将一个客户的凭据、数据、知识库、输出或操作带入其他客户环境。

主体

主要责任

在约定服务范围内提供已正式发布并启用的能力，并依据适用文件实施相应的服务、GloryScience 安全、支持和风险控制；可依主协议及适用文件对异常、高风险或违规使用采取限制、暂停、降级或其他合理措施。

用户应为生产网络连接、外部执行、自动化和高影响用途指定具备相应权限、知识和内部授权的责任人。

智能体输出、展示、告警、推断、建议或对话内容，不当然等同于现场事实、用户批准、设备厂商结论、正式工单、审计结论、合规结论或已经完成的执行。

用户对其最终业务决策、内部审批和生产网络变更承担控制责任，但前述责任分配不排除或限制 GloryScience 根据主协议、适用 DPA、Security Addendum、其他书面文件或强制性法律承担的义务，也不免除 GloryScience 因其自身违约、故意不当行为或重大过失依法或依约应承担的责任。

4. 能力范围与统一限制

4.1 实际可用范围

智能体能力的实际可用范围取决于用户订阅或试用、服务地区、产品版本、角色权限、已接入数据、知识来源、功能开关、第三方依赖和当前服务状态。

Oneasy 官方网站、品牌材料、演示、销售介绍、路线图、概念名称或智能体自身回答，不构成未订购功能、特定模型、特定知识库、特定接口、特定设备兼容、特定准确率、服务结果或持续可用性的承诺。

4.2 智能体治理分类

以下分类用于说明治理边界，不单独证明具体能力已经发布或包含于用户订阅：

智能体或能力类别	在正式发布并启用时可能涉及的用途	特别边界
AI Assistant / Oneasy 智能辅助	Oneasy 产品与网络运维问答、平台知识与界面引导、经批准的业务查询、结果总结、可视化、知识检索及诊断流程辅助	仅可使用正式开放的页面、接口、数据和权限；不得臆造接口、参数、设备状态或执行结果。
OnExpert	专家知识、网络运维知识检索、诊断思路和经验辅助	仅在正式发布并启用时适用；不构成设备厂商认证、官方支持结论、兼容性承诺或生产变更指令。
OnTwin	可视化、状态理解、对象关系或影响分析等辅助能力	仅在正式发布并启用时适用；展示、模型或推断不当然等同于现场真实状态、资产清单、验收结论或完整数字孪生。

如产品界面、发布说明或订单使用不同名称，应以对应正式文件和实际启用状态为准。

4.3 智能体固有限制

用户理解，智能体输出由用户输入、租户数据、知识来源、模型能力和系统配置自动或半自动生成，可能存在：

- 信息不完整、不准确、过时或与当前版本不一致；
- 误判、遗漏、幻觉、推理错误或不确定性；
- 设备型号、软件版本、MIB、OID、CLI、API、数据模型或现场环境差异；
- 上下文不足、数据缺失、接口返回异常或权限导致的可见范围限制；
- 第三方模型、知识库、云服务或外部接口造成的限制。

智能体输出仅用于辅助信息检索、理解、分析、诊断、可视化、操作指引和方案草拟，不替代具备相应权限和能力的工程师、安全人员、管理人员、法务或合规人员的最终判断。

5. 数据、账户、知识库与第三方服务

5.1 合法授权与数据最小化

1. 用户仅可提交、授权处理或连接其拥有合法权利，且已完成必要告知、同意、授权、审批或其他合法程序的数据、网络、设备、系统和第三方技术资料。
2. 用户应遵循目的限定、数据最小化和最小权限原则。日志、配置、截图、工单、抓包或诊断材料应删除与任务无关的个人数据、凭据和敏感信息。
3. 用户不得以智能体能力规避其作为数据控制者、数据使用者、网络运营方或其他责任主体依法应履行的告知、授权、评估、备案、保密或安全义务。
4. 用户为合法的网络运维、支持、安全或合规目的处理相关信息时，仍应遵守主协议、适用 DPA、数据最小化、目的限定和访问控制要求。

5.2 凭据与敏感信息

1. 不得在普通对话、提示词、知识库、普通附件或不受控文件中提交完整密码、私钥、访问令牌、API Key、VPN、SSH、SNMP 高权限凭据、支付凭据或其他不应进入模型上下文的信息。
2. 产品功能确需使用接入凭据时，用户应通过 Oneasy 明确指定的受控凭据管理通道提交，并按照正式产品说明配置最小权限、有效期限、轮换、撤销和访问控制。
3. 除非正式产品说明、适用合同和服务配置明确允许，不得假设通过受控凭据通道提交的凭据会被提供给智能体模型或进入普通对话、知识库和不受控日志。
4. 用户应采取与风险相称的账户安全、强认证（在产品支持时）、RBAC、凭据轮换、离职或转岗后的权限回收及日志审查措施，不得共享管理员账户或允许未授权人员使用账户。

5.3 第三方模型与数据处理

1. Oneasy 的部分智能体能力可能使用第三方大型语言模型、模型 API、嵌入模型、向量数据库或其他 AI 服务。
2. 具体服务商、处理目的、数据类别、处理地点、保留安排、子处理者和跨境传输机制，以适用 DPA、子处理者清单、隐私政策、AI 数据说明、订单、服务配置或其他正式文件为准。

3. 除非获得用户明确书面授权，GloryScience 不会使用可识别的用户数据训练面向其他客户或公众的通用人工智能基础模型。
4. 前款“不用于训练”的约定，不表示用户输入、附件、查询结果或相关上下文绝不会由第三方 AI 服务为推理、嵌入、检索、安全监控或提供功能所必要的其他目的进行处理。相关处理仍受适用文件和数据保护要求约束。
5. 用户不得提交其无权提供给 GloryScience 或相关第三方 AI 服务处理的数据、保密信息或受监管信息。

5.4 受保护数据

未经适用合同、产品配置和合法依据明确允许，用户不得提交：

- 原始通信内容或受通信保密义务保护的信息；
- 国家秘密或法律禁止跨境、外包或向第三方处理的信息；
- 未经授权的受限商业秘密；
- 高度敏感个人数据或其他受严格监管数据；
- 任何用户无权向 GloryScience 或第三方模型服务商披露的信息。

确需处理受保护数据时，用户应事先确认合法依据、适用 DPA 或专项文件、数据区域、权限、保留和安全控制均满足其要求。

5.5 知识库、提示词与第三方技术资料

1. 用户管理员应管理知识库和提示词的来源、权利状态、适用范围、版本、更新责任、访问角色和失效内容。
2. 用户上传或要求使用设备厂商资料、MIB、OID、CLI/API 文档、固件资料、配置模板、抓包、日志样本或其他第三方技术资料时，应确保具有合法取得、披露、复制、上传、处理和授权使用的权利。
3. 用户不得上传来源不明、受保密义务限制、受设备厂商许可限制或可能侵犯第三方知识产权、商业秘密、合同权利、通信保密义务或其他合法权益的资料。
4. 知识库内容、检索片段和模型回答不当然构成最新、完整或具有官方效力的设备厂商资料。涉及具体型号、软件版本、命令、参数或配置时，应核对正式资料和现场条件。
5. 用户自有提示词、知识库材料及其他用户内容的权利，适用主协议第六条；本规范不改变主协议关于知识产权、用户内容和 GloryScience 专有系统提示词、模板、工作流及平台能力的安排。

5.6 提示词注入与第三方连接

1. 网页、文件、邮件、检索结果、第三方工具、设备返回内容或用户输入中的指令性内容可能不可信。
2. 用户不得利用该等内容诱导智能体泄露信息、改变权限、绕过规则、跨租户访问或执行未授权操作。
3. 新增或变更第三方工具、系统、设备、数据源、接口、插件或自动化时，用户应明确业务目的、数据范围、最小权限、使用人、责任人、风险、停止方式和退出方式。

4. 不再需要、授权被撤销、人员离职、凭据异常或发现风险时，用户应及时限制、撤销或轮换相应连接和凭据。

5.7 租户隔离与记录

1. 用户不得尝试访问其他租户、未获授权的内容、平台管理能力、日志、接口、凭据或系统资源。
 2. 发现跨租户可见、异常权限或非预期数据访问时，应立即停止相关操作并通过指定支持或安全入口报告；不得通过继续查询、批量下载、截图传播、转发或扩大测试范围增加影响。
 3. 用户管理员应对账号、角色、知识库、连接、自动化和高影响配置的新增、调整、停用或撤销，保留与风险相称的客户级记录。
 4. 智能体对话记录不能替代用户内部所需的审批单、工单、变更单、授权记录、现场记录或其他受控证据。
-

6. 生产网络、外部执行与高风险网络操作

6.1 基本原则

对 OLT、ONU、CPE、端口、VLAN、QoS、ACL、认证、路由、业务模板、批量开通或配置、脚本、自动化任务、固件、远程命令及其他可能影响生产网络或终端用户服务的事项，智能体输出仅可作为候选方案、分析、建议或草稿。

智能体输出不得直接视为已批准、已执行、可直接投产的操作指令或对执行结果的保证。

6.2 执行前人工复核

执行高风险网络操作前，用户应由具备相应权限和能力的人员至少核验：

- 目标设备、对象、租户、站点和影响范围；
- 设备厂商、型号、软件或固件版本；
- 网络拓扑、业务依赖和当前运行状态；
- 命令、脚本、参数、模板和接口语义；
- 预期结果、失败条件、停止条件和回滚方式；
- 内部审批、测试验证、配置备份、维护窗口、现场值守、终端用户通知及监管要求。

对重大、批量、跨区域、删除、停机、固件、权限、不可逆或可能中断业务的操作，用户应按照其内部制度实施更严格的复核和审批。

6.3 外部执行授权

1. 是否提供外部执行能力，以相关功能已经正式发布、包含于用户订阅、在用户租户中启用并通过正式产品说明明确为准。
2. 除非订单、产品配置或双方书面文件明确允许，用户应将智能体外部执行视为未启用或不被允许。

3. 智能体对话、自然语言指令、“执行”“继续”等一般性表述、参数预填、模型建议或建议采纳，不单独构成有效的生产执行授权。
4. 外部执行应通过产品提供的独立受控机制或用户批准的外部系统流程完成，并满足适用的身份验证、角色权限、内部审批、执行确认和审计要求。
5. 在产品支持的范围内，用户应对重大或高风险操作启用二次确认、提升认证、申请人与批准人分离或双人批准等控制。
6. 用户不得利用智能体绕过网络隔离、变更审批、权限控制、维护窗口或现场安全控制。

6.4 执行范围、记录与停止

1. 自动化或外部执行任务应具有明确目标、对象、范围、最小权限、有效期限、停止或撤销机制、执行记录和结果验证。
2. 用户应避免将开放式、含糊或无边界的自然语言指令直接转化为生产执行。
3. 在产品提供相应记录能力时，用户应结合产品日志和自身受控记录，区分人工发起、API 发起、定时任务、系统自动任务、智能体建议及实际执行。
4. 用户应确保存在可用的任务终止、凭据撤销、连接断开、配置回滚或其他紧急停止路径；具体能力以产品版本、设备适配和现场条件为准。
5. 执行后应核验设备实际返回结果、业务状态、影响范围、失败对象和回滚结果，不得仅以智能体文本或对话结论作为完成证明。

6.5 异常处置

发生异常、结果与预期不符、影响范围不明、权限异常、跨租户可见、数据误披露、危险输出已被执行或可能被执行时，用户应：

1. 立即停止后续操作或高风险任务；
2. 按用户内部事件流程采取隔离、断开、回滚、凭据撤销或轮换等措施；
3. 保留必要日志、时间、对象、版本、指令和执行结果；
4. 通过 Oneasy 指定支持或安全入口报告；
5. 配合 GloryScience 在合理范围内开展调查、缓解和恢复。

7. 禁止用途

用户不得利用智能体能力，亦不得指使、授权、协助或默许他人：

1. 未经授权访问、扫描、测试、控制、干扰、攻击、规避安全控制或获取任何网络、设备、账户、数据或凭据；
2. 生成、传播或执行恶意代码、钓鱼、欺诈、勒索、拒绝服务、凭据窃取或其他违法有害活动；
3. 违反电信监管、网络安全、通信保密、数据保护、出口管制、制裁、知识产权或其他适用法律；
4. 在缺乏合法依据、必要授权或适用文件允许的情况下，上传、推断、披露、关联或再识别他人的个人数据、通信内容、商业秘密或其他受保护信息；
5. 冒充他人，或伪造设备状态、操作记录、审计证据、测试结果、合规结论、厂商意见、现场操作或正式授权；

- 6. 规避订阅、调用额度、权限、计费、日志、审计、风控、内容限制或其他技术和合同控制；
- 7. 将智能体输出作为医疗、法律、金融、监管、合同、公共安全或其他高影响事项的唯一或最终依据；
- 8. 未经必要授权、人工审核、审批、测试、备份和回滚安排，将智能体输出直接用于生产网络高风险操作；
- 9. 试图套取、泄露或绕过 Oneasy 专有系统提示词、安全规则、模型配置、访问控制、租户隔离或其他保护措施；
- 10. 上传、使用或要求处理无权披露、无权复制、受保密义务或设备厂商许可限制的第三方技术资料；
- 11. 反向工程、反编译、篡改、绕过、未经授权复制或二次分发 Oneasy 智能体、网络接入组件、接口、专有系统提示词或相关安全控制，但适用法律强制允许或 GloryScience 明确书面授权的除外；
- 12. 将智能体输出、产品名称或兼容结果误述为 GloryScience、Oneasy、设备厂商或任何第三方已经作出的正式意见、认证、背书、承诺、报价、审批、验收或授权。

本条与主协议第四条、第五条及其他禁止行为条款累积适用。

8. 人工复核、输出使用与对外发布

场景	最低要求
一般问答、操作说明、文本或表格草稿	核对关键事实、产品版本、适用范围和明显错误后使用。
故障分析、根因推断、设备兼容、配置、命令或脚本建议	由熟悉相关网络、设备和现场条件的人员交叉验证；核对正式资料、版本、日志和实际返回结果；保留未确认事项。
生产变更、批量任务、远程接入或外部执行	按第6条完成授权、人工复核、审批、测试、备份、维护窗口、执行确认、结果验证和必要记录。
安全事件、数据泄露、重大中断、监管或合同事项	立即进入用户指定的安全、管理、法务或合规路径；智能体输出不得替代正式调查、决定、通知或报告。
对外发布、报价、合同、报告、审计或验收材料	完成事实、来源、权利、授权和内部审批核验；清晰区分草稿、建议、推断与正式结论。

用户不得删除、遮挡或误导性修改产品提供的 AI 身份、生成内容、风险提示或来源提示标识。

用户引用或使用智能体输出时，应保留其辅助性质，并自行核验引用来源、事实、第三方权利和适用性。本规范不改变主协议关于知识产权、用户内容、AIGC、反馈及第三方权利的安排。

9. 试用、资源与功能调整

- 1. Trial、Beta、Preview、Free、Early Access 或推广期智能体能力，仅在当期订单、试用规则、产品页面、后台展示或双方书面文件明确的范围内提供。

2. 可用功能、调用次数、Token、计算资源、数据范围、知识库、模型、第三方依赖或并发可能受配额、地区、租户状态、风险控制、合理使用和技术条件限制。
 3. 除非订单、Enterprise SLA 或其他书面文件另有约定，试用、免费或预览能力不构成 SLA、持续可用性、性能、功能稳定性或长期免费承诺。
 4. GloryScience 可因安全、法律、服务稳定性、滥用防控、供应商依赖、资源公平使用或产品迭代需要，对相关能力进行限流、降级、暂停、替换、移除或调整。
 5. 对可能对用户权利产生实质性不利影响的变更，适用主协议的通知规则；因紧急安全、法律、监管或服务连续性原因需要立即处置的除外。
 6. GloryScience 采取限制或暂停措施时，可在风险允许和商业合理范围内将措施限制在必要范围，并在风险解除、用户完成必要整改或替代控制得到确认后，对恢复相关能力进行合理复核。本条不构成固定恢复时限或 SLA。
-

10. 支持、事件、纠错与申诉

10.1 支持与纠错

用户应使用 Oneasy 平台、订单或官网指定的支持渠道报告问题。本规范不单独设定支持时段、响应时间、解决时限或 SLA。

用户或授权用户可报告错误输出、误拒绝、权限、数据、配置或服务使用问题，并可请求人工复核或纠错。提出纠错或申诉不表示相关输出、操作、授权、对外发布或业务决定已经自动撤销；用户仍应依问题性质完成暂停使用、人工复核、对外修正和内部补救。

10.2 事件报告

用户发现下列情况时，应尽快报告：

- 账户、凭据疑似泄露或异常登录、异常调用；
- 跨租户可见、异常权限或非预期数据访问；
- 危险输出已被执行或可能被执行；
- 数据误提交、误披露、误删除或被错误用于智能体处理；
- 远程接入、接口、工具调用或外部执行异常；
- 其他可能影响网络、数据、用户或服务安全的事件。

报告应在不披露额外敏感凭据的前提下，尽可能提供租户信息、联系人、发生时间、受影响范围、相关功能、模型或版本（如已知）、已采取措施及可供调查的日志、任务编号或截图。

用户应及时采取本地隔离、停止任务、撤销或轮换凭据、断开连接、回滚和其他必要缓解措施，并配合合理调查。

10.3 风险处置

在合理认为存在安全、法律、滥用、数据保护、第三方服务、生产网络或业务连续性风险时，GloryScience 可依主协议及适用文件暂停、限制、撤销或降级相关账户、智能体能力、API、网络接

入组件、远程接入或其他相关功能。

10.4 联系方式

- 一般咨询与技术支持：service@oneasy.cc
 - 法律与数据保护事项：legal@oneasy.cc
 - 安全事件：Oneasy 平台、订单、官网指定的安全或支持入口
-

11. 更新、接受与生效

11.1 首次并入与生效

本规范仅在被明确引用并由用户或其授权代表通过可记录方式接受后，构成主协议的一部分。可记录方式包括：

- 点击同意或勾选确认框；
- 在订单、Subscription Order、SOW 或其他书面文件中明确引用并接受；
- 在管理后台或智能体功能首次启用流程中完成确认；
- 其他能够证明用户知悉本规范名称、版本并作出接受的方式。

仅访问未明确引用本规范的网页、仅保存支付信息或仅使用与智能体无关的服务，不当然构成对本规范的接受。

11.2 已接受版本的更新

GloryScience 可不时更新本规范。非实质性修改可通过更新版本号、最后更新日期或发布说明生效。

对于可能对用户权利产生实质性不利影响的修改，GloryScience 将按照主协议及适用法律的通知规则办理。用户在通知期届满且新版本生效后继续使用适用的智能体能力，表示接受更新后的本规范。

因紧急安全、法律、监管、第三方服务或服务连续性原因需要立即采取措施的，GloryScience 可先行限制或调整相关能力，并在合理可行范围内补充通知。

11.3 接受记录

GloryScience 可为合同、审计、安全和争议处理目的，记录适用的规范版本、接受时间、租户、管理员或授权代表、接受动作及相关技术记录。该等记录的处理应遵守主协议、隐私政策、适用 DPA 和法律要求。

11.4 语言

如本规范存在多个语言版本，适用的控制语言以订单、正式发布页面或双方书面文件为准。未指定的，以简体中文版本为准。

12. 附录的性质

附录 A、附录 B 和附录 C 用于协助用户建立内部治理、配置、变更和复核流程。

除非订单、SOW、Enterprise SLA 或双方专项书面文件另有明确约定：

- 1. 附录中的检查表、模板和建议不单独扩大 GloryScience 的服务义务、功能承诺、SLA 或责任范围；
- 2. 附录中提及的控制不表示相关产品功能在所有版本、套餐或租户中均已提供；
- 3. 用户未逐项采用某项建议，不当然构成违约，但用户仍应履行主协议、本规范及适用法律明确要求的义务；
- 4. 用户应根据其业务规模、网络风险、监管环境和内部制度决定适用的控制强度。

附录 A：客户管理员上线与配置检查表

检查项	建议确认内容
客户与租户	用户主体、租户、管理员、授权代表和有效支持入口已确认。
账号与角色	用户、角色、最小权限、管理员权限、离职或变更处理方式已确认。
产品与范围	已订购、已发布、已启用的智能体能力、用户范围、禁止场景和已知限制已确认。
数据与知识库	数据来源、合法依据、知识库范围、权利状态、访问角色、更新和失效责任已确认。
第三方模型与连接	已了解适用的数据说明、第三方模型或子处理安排；第三方连接、权限、数据范围和退出方式已确认。
凭据管理	普通对话与受控凭据通道已经区分；凭据最小权限、轮换、撤销和日志审查方式已确认。
外部执行	是否提供、是否启用、授权人、审批流程、执行确认、停止和回滚方式已确认。
高影响事项	人工复核、客户授权、生产边界、测试、备份、维护窗口和结果验证方式已确认。
支持与事件	正式支持入口、客户联系人、升级、事件报告和本地缓解方式已确认。
定期复核	账号、权限、知识库、连接、模型或功能变化后的复核安排已确认。

附录 B：重大变更与集成申请要素

字段	填写或确认内容
基本信息	申请标识、日期、申请人、责任人、变更或集成名称与目的。
影响范围	产品、租户、用户、系统、设备、站点、数据和第三方服务。
变更类型	知识库、提示词、工作流、工具、接口、权限、模型、自动化、外部执行、生产环境、公开内容或其他。

字段	填写或确认内容
数据与权限	数据类别、合法依据、访问角色、最小权限、凭据方式、处理区域和退出方式。
风险与授权	已知限制、高影响事项、用户责任人、适用内部批准和第三方授权。
测试与验证	测试范围、环境、设备或版本、验证人、结果、遗留问题和处置。
执行控制	独立确认、身份验证、审批、执行窗口、影响范围和记录方式。
回退与停止	回退、降级、紧急停止、凭据撤销或断开方式、触发条件、责任人和验证方式。
决定记录	批准、拒绝或条件批准；日期、条件、有效期限及关联受控记录。

附录 C：按智能体类别适用的补充规则

本附录中的名称仅用于治理分类，不构成功能已经发布、包含于订阅或可持续使用的承诺。

智能体或能力类别	补充规则
AI Assistant / Oneasy 智能辅助	文件、知识库、草稿、报告、邮件、代码、表格、查询结果或图表用于高影响业务、对外发布、正式承诺或专业判断前，应由具备权限的人员核验和批准。查询和分析仅应基于正式开放的接口及实际返回数据。
OnExpert（如正式发布并启用）	用户应提供尽可能准确的设备、版本、时间、症状、日志和环境信息；对诊断、引用、工单和报告，应核验事实、假设、来源和不确定性，不得伪造设备厂商意见、现场操作或验收证据。
OnTwin（如正式发布并启用）	对可视化、状态、对象关系、趋势、仿真或影响分析，应核验数据完整性、时间戳、对象标识、采集范围和适用条件；不得因未出现告警或模型显示正常而取消必要巡检、现场核验或应急措施。

发布主体： GloryScience International Limited
注册地址： NEW TREND CTR, NO. 704 PRINCE EDWARD RD EAST, SAN PO KONG, HONG KONG
法律联系邮箱： legal@oneasy.cc
服务支持邮箱： service@oneasy.cc

修订记录

版本	日期	说明
V1.0	2026年7月27日	初始版本。

版本	日期	说明
V1.1	2026年7月27日	明确本规范作为主协议智能体服务专项附录的法律性质；完善首次并入与更新机制、功能可用性边界、第三方模型与数据处理说明、凭据通道、外部执行授权、高风险网络操作、责任保留及附录指导性质。