Oneasy Security Addendum

Oneasy 安全附录（国际企业增强版）

最后更新日期： 2026年6月25日
生效日期： 2026年6月25日

---

1. Purpose and Scope

第一条 目的与适用范围

本《Security Addendum》（“本安全附录”）是《Oneasy SaaS 服务协议》的补充文件，旨在说明 **GloryScience International Limited** 通过 Oneasy SaaS Platform（“Oneasy”）为保护客户数据、租户数据、平台运行数据及相关系统安全所采取的技术与组织安全措施。

为避免疑义，本安全附录中，“GloryScience”指 GloryScience International Limited；“Oneasy”或“Oneasy 服务”指由 GloryScience 提供和运营的 Oneasy SaaS Platform、相关功能、组件、API、Agent/VPN 接入能力及支持服务。除描述产品、平台、功能或技术组件外，本安全附录项下的权利、义务、责任限制和客户通知义务均由 GloryScience 享有或承担。Oneasy 不应被解释为电信运营商、ISP、客户网络运营者、客户终端用户通信服务提供者或客户生产网络的最终控制方。

本安全附录适用于 Oneasy 通过 SaaS 模式向客户提供的云端智能运维平台、API、管理后台、远程接入组件、Agent/VPN 接入能力及相关支持服务。

如本安全附录与主协议存在冲突，就安全控制、安全事件响应、访问控制、技术与组织安全措施、Agent/VPN/远程接入安全、漏洞管理、日志保留、AI 安全和客户安全责任等事项，以本安全附录为准；如该等事项同时涉及个人数据处理、跨境传输、子处理者、数据主体请求、个人数据泄露通知或数据保护法律义务，则 DPA 中的专门约定优先适用。其他事项仍以主协议为准。

---

2. Security Governance

第二条 安全治理

GloryScience 将建立并维护商业合理的信息安全管理机制，包括：

1. 指定安全管理责任人或安全管理团队；
2. 制定内部安全管理制度、访问控制流程和事件响应流程；
3. 对涉及客户数据访问的员工、承包人员或其他授权人员施加保密义务；
4. 定期评估平台安全风险，并根据业务发展、威胁变化、技术条件和客户合理需求持续改进安全控制措施；

5. 在合理范围内参考 ISO 27001、SOC 2、CSA CCM 等行业通行安全原则。

除非 Oneasy 已取得正式认证，本安全附录中对 ISO 27001、SOC 2、CSA CCM 或其他标准的引用仅表示安全控制参考，不构成 Oneasy 已通过该等认证、审计或保证的声明。如 Oneasy 未来取得相关认证、报告或第三方评估，应以实际证书、审计报告、适用范围和有效期间为准。

---

3. Data Hosting and Segregation

第三条 数据托管与租户隔离

1. 默认情况下，Oneasy 的主要云托管、主要数据处理与主要存储区域位于阿里云国际云新加坡区域。GloryScience 可根据服务可用性、灾难恢复、安全防护、技术支持、性能优化、子处理者服务或客户配置，在其他区域设置从节点、灾备节点、边缘节点、日志节点或支持访问节点。
2. GloryScience 将通过 Oneasy 服务采用逻辑隔离机制区分不同客户的租户空间、账户、权限及数据。
3. GloryScience 将采取合理措施，防止未经授权的跨租户访问。
4. 客户应自行负责其租户内的用户管理、角色分配、权限配置及内部访问审计。
5. 若客户要求特定数据区域、数据本地化、跨境传输限制、专属环境、专属密钥或额外隔离措施，应通过 Order Form、SOW、DPA、SLA 或专项协议另行约定，并可能产生额外费用。

---

4. Access Control

第四条 访问控制

GloryScience 将通过 Oneasy 服务采取商业合理的访问控制措施，包括：

1. 基于角色的访问控制（RBAC）；
2. 最小权限原则；
3. 员工访问权限审批与回收机制；
4. 对生产系统访问进行限制；
5. 对高权限操作进行记录；
6. 在技术可行范围内支持多因素认证（MFA），并对内部高权限账户、生产环境访问账户或其他高风险账户适用更严格的身份认证控制；
7. 定期或在人员变动、职责调整、权限异常或安全事件后审查内部访问权限；
8. 对访问凭据、API Key、访问令牌、VPN/Agent 凭据及其他敏感认证信息实施合理保护措施。

客户负责：

1. 妥善管理其管理员账户；
2. 为授权用户分配适当权限；
3. 及时移除离职、转岗或不再需要访问权限的用户；

4. 妥善保管密码、API Key、访问令牌、VPN/Agent 凭据等敏感凭证；
5. 在 Oneasy 支持相关功能时，为管理员账户和高权限用户启用 MFA 或其他强认证措施；
6. 对客户自身账户被盗用、共享账户、弱密码、凭据泄露或权限配置不当导致的风险承担责任。

---

5. Encryption and Sensitive Data Protection

第五条 加密与敏感数据保护

GloryScience 将根据行业通行安全实践、服务场景及合理商业标准，通过 Oneasy 服务采取适当的技术与组织措施保护数据安全，包括但不限于：

1. 对传输中的数据使用行业通行的加密传输协议。在技术可行且适用的场景下，GloryScience 将通过 Oneasy 服务优先采用 TLS 1.2 或更高版本，或同等级安全协议；
2. 在适用场景下，对生产环境中的静态数据采取合理的加密、隔离、访问控制或等效保护措施；
3. 对密码、访问凭据、密钥、令牌及其他敏感认证信息采取合理保护措施，包括哈希、加密、安全存储、访问限制或其他等效安全措施；
4. 尽合理努力避免在日志、错误信息、调试输出、普通文本配置、客户支持沟通或非安全渠道中暴露完整敏感信息；
5. 根据合理安全实践，对敏感数据访问实施适当的访问控制、权限限制和审计记录；
6. 在商业合理范围内，对密钥、证书、令牌及敏感凭据实施生命周期管理，包括生成、存储、访问、轮换、撤销和删除。

GloryScience 可根据技术发展、安全风险、行业标准更新、第三方依赖变化或服务架构调整，更新或调整相关安全措施，但不会有意降低本安全附录所描述的总体安全保护水平。

客户应避免通过非指定字段、普通支持渠道、即时通讯、非安全邮件或其他非安全方式提交明文密码、私钥、未脱敏敏感个人信息、非法监听数据、未授权通信截获数据或其他高风险敏感数据。

除双方另有书面约定外，GloryScience 不承诺满足特定行业、特定国家、特定监管框架、特定加密算法认证或专属密钥管理方案下的专门要求。

---

6. Logging and Monitoring

第六条 日志与监控

GloryScience 将根据合理安全实践、服务运营需要、合规要求及 Oneasy 服务的实际功能，维护适当的日志与监控机制，用于平台运行监控、安全事件检测、故障排查、异常访问分析、审计支持和合规记录。

相关日志可能包括登录与认证记录、API 调用记录、关键操作记录、系统错误与运行日志、安全事件相关日志、Agent/VPN 或远程接入连接状态与访问记录，以及高风险配置变更、自动化任务、批量任务或远程运维操作的相关记录。

GloryScience 将在商业合理范围内采取适当措施，降低日志被未经授权访问、篡改、异常删除或不当导出的风险。相关措施可包括访问控制、权限限制、完整性保护、备份、集中化日志管理、时间戳记录或其他等效控制。

日志的具体类型、记录粒度、保留期限、访问方式和导出能力，可能因服务版本、部署方式、系统配置、数据类型、安全风险、法律要求和客户所订购的服务范围而有所不同，并以主协议、DPA、Security Addendum、Order Form、系统配置或适用法律要求为准。

除适用法律另有强制要求或双方另有书面约定外，GloryScience 无义务长期保存历史日志、提供完整原始系统日志、满足司法取证标准，或提供超出合理运营、安全支持和合规需要范围的日志访问。

在适用法律要求或合理合规需求下，GloryScience 可在合理范围内配合客户处理与安全事件、监管要求或审计相关的日志支持请求。GloryScience 可根据安全、保密、其他客户权益、系统完整性、商业秘密或法律限制，对相关日志内容进行合理脱敏、汇总、截取或访问限制。

如日志、抓包文件、配置备份、CLI 输出、API 返回、Agent/VPN 诊断文件或其他排障材料中可能包含第三方设备厂商专有资料、客户商业秘密、网络安全敏感信息或受监管数据，GloryScience 可在商业合理范围内对相关内容进行脱敏、截取、限制导出、隔离存储或删除，并可基于安全、保密、第三方权益、知识产权、商业秘密或适用法律要求限制相关内容的访问、共享、复制或下载。

---

7. Network and Infrastructure Security

第七条 网络与基础设施安全

GloryScience 将采取合理的网络与基础设施保护措施，包括：

1. 网络访问控制；
2. 防火墙、安全组或等效隔离措施；
3. 云基础设施安全配置；
4. 安全补丁与漏洞修复流程；
5. 生产环境与非生产环境的合理隔离；
6. 关键组件的容量、可用性和安全监控；
7. 防范恶意访问、异常流量、暴力破解、权限滥用和服务滥用的合理技术措施；
8. 在适用场景下，对管理接口、API、后台入口、远程接入入口及高风险组件实施访问限制或增强监控。

Oneasy 服务的部分基础设施可能依赖第三方云服务商、网络服务商、安全服务商、监控服务商、通信服务商或其他第三方服务商。GloryScience 将采取商业合理措施选择具备适当安全能力的服务提供商，并通过合同、供应商管理或其他合理机制约束其安全责任。

---

8. Agent / VPN / Remote Access Security

第八条 Agent、VPN 与远程接入安全

由于 Oneasy 可能通过 Agent、VPN、Connector、API、隧道、远程脚本、运维工具或其他远程接入方式连接客户网络环境，双方确认该场景具有较高安全敏感性，并可能涉及对客户网络设备、OLT/ONU 管理接口、配置系统或运维环境的访问。

Oneasy 的远程接入能力应默认遵循客户授权、目的限定、最小权限、最小网络暴露、可撤销、可审计和安全可控原则。

8.1 Access Establishment and Authorization

8.1 接入建立与授权

1. 远程接入应基于客户接受主协议、本安全附录、服务配置、Order Form、实施方案、后台配置、管理员操作、产品内确认或其他双方认可的方式建立。
2. 客户点击接受主协议或本安全附录、添加设备、配置凭据、启用 Agent / VPN / Connector / API / SNMP / TR-069 / TR-369 / CLI / Syslog / ACS / NMS 接口、上传或提交 MIB、OID、SNMP walk 结果、CLI/API 输出、配置备份、日志、抓包文件、脚本、模板、设备资料、厂商资料或其他第三方技术资料，或以任何方式请求 GloryScience 提供相关支持的，即视为客户已授权 GloryScience 在提供、运行、维护、保护、支持、诊断、适配、测试、改进和优化 Oneasy 服务所必要或合理相关的范围内接入、读取、采集、解析、缓存、处理、展示、分析、调用、下发或协助操作相关设备、系统、接口、账户、凭据、数据和运维环境。
3. 客户应确认其对相关 OLT、ONU、CPE、ACS、NMS、网络、接口、账户、凭据、数据、日志、配置、拓扑、客户网络数据和第三方技术资料，拥有充分的所有权、运营权、管理权、授权运维权、合同授权、内部审批、第三方许可、设备厂商许可、保密豁免、监管许可、终端用户告知或同意，或其他合法依据。
4. 除双方另有书面约定外，GloryScience 不会通过 Oneasy 服务主动接入客户未授权的网络、系统、设备或数据。GloryScience 有权合理依赖客户在主协议、本安全附录、服务配置、上传记录、授权读取记录、管理员操作、产品内确认、工单或其他服务内指令中作出的声明、保证、授权和操作记录。
5. 客户可通过管理后台、配置变更、网络策略、凭据撤销、VPN 关闭、书面通知或其他合理方式暂停、限制或撤销远程接入；但该等撤销不影响撤销前已根据客户授权进行的处理活动的合法性，也不影响 GloryScience 基于安全、审计、备份、争议保全、法律义务或合理运营需要对必要记录进行留存。

8.2 Access Scope and Network Boundary

8.2 接入范围与网络边界

1. 除双方另有书面约定外，远程接入仅限提供服务所必要的 OLT/ONU 管理接口、协议、端口、账户、网段、日志、遥测、配置或运维数据。
2. 远程接入不得被用于客户办公网、财务系统、人力资源系统、终端用户业务流量内容、非服务目的内部系统或与 Oneasy 服务目的无关的环境访问。

3. 客户应通过网络隔离、防火墙、安全组、ACL、白名单、路由策略、跳板机、专用账户或其他措施限制 Agent/VPN 可访问范围。
4. 在技术可行且适用的部署模式下，Agent 或 Connector 宜优先采用客户侧发起的加密出站连接、客户批准的 VPN 隧道或其他降低暴露面的接入方式。
5. 如客户要求开放公网端口、弱隔离网段、共享账户、过高权限账户或超出服务目的的访问范围，应由客户承担相应风险，并可能需要双方另行书面确认。

8.3 Credential and Key Management

8.3 凭据与密钥管理

1. 客户应负责创建、配置、保管、轮换和撤销其提供给 Oneasy 或在 Oneasy 中配置的客户侧账户、SNMP community、API Key、Token、VPN 凭据、设备账号、私钥、证书或其他敏感凭据。
2. GloryScience 将在商业合理范围内保护由 GloryScience 通过 Oneasy 服务管理或存储的远程接入凭据，避免以普通明文方式暴露完整敏感凭据。
3. 对由客户控制的设备账户、网络账户、VPN 账户或本地系统账户，客户应根据自身安全政策定期轮换，并在人员变动、授权范围变化、服务终止、疑似泄露或安全事件后及时撤销或更换。
4. 除双方另有书面约定外，客户不得向 Oneasy 提供共享管理员账户、无法审计的通用账户、超出服务目的的高权限账户或与服务无关的生产系统凭据。
5. 客户不得将来源不明、无权披露、无权授权使用、受第三方保密限制或明确禁止云端处理的 MIB、OID、SNMP walk 结果、CLI/API、OMCI、固件资料、设备厂商内部文档、私有接口说明或其他第三方技术资料，伪装为凭据、配置参数、支持材料、备注、脚本或诊断文件提交至 Oneasy。客户在有权提供或有权授权读取该等资料的情况下，通过 Oneasy 服务提交、配置、上传、授权读取或允许生成该等资料的处理，应适用第 8.4 条。

8.4 Technical Materials and Vendor Materials Security

8.4 技术资料与设备厂商资料安全

为本安全附录之目的，**第三方技术资料（Third-Party Technical Materials）** 指客户、渠道伙伴、设备厂商、代理商、系统集成商、供应商或其他第三方向 GloryScience 或 Oneasy 提供、上传、传输、展示、披露、引用、授权读取、允许生成或要求使用的任何设备、网络、协议、接口或厂商资料，包括但不限于 MIB 文件、OID 表、SNMP walk 结果、CLI/API 文档或输出、命令手册、私有接口说明、OMCI 资料、基于 TR-069 / TR-369 / TR-181 或其他公开标准形成的厂商私有扩展、非公开参数、私有数据模型、ACS/NMS 接口文档、固件说明、配置模板、脚本、抓包文件、日志样本、厂商支持资料、设备测试报告、兼容清单、供应商保密资料或其他可能受知识产权、商业秘密、合同限制或保密义务保护的资料。

为避免疑义，公开发布的行业标准、公开协议规范、公开 RFC、Broadband Forum 公开发布的 TR-069、TR-369、TR-181 技术报告或数据模型，以及其他合法公开资料本身，不因 Oneasy 支持、引用、实现、解析或适配而当然构成第三方保密资料或受保护第三方技术资料。但该等公开资料的使用仍应遵守其适用的版权声明、许可条款、使用条件或标准组织规则。

厂商、客户、系统集成商或其他第三方基于公开标准形成的私有扩展、非公开参数、非公开实现说明、厂商内部文档、私有 MIB/OID、私有 CLI/API、设备输出结果、客户现场配置、日志、抓包、SNMP walk 结果、诊断结果或其他非公开资料，仍可能构成客户数据、客户网络数据、第三方技术资料、商业秘密、保密资料或受合同限制资料。

客户通过 Agent、VPN、Connector、API、支持工单、日志上传、抓包文件、配置备份、CLI 输出、诊断文件、脚本、配置模板或其他方式向 Oneasy 提交、上传、配置、授权读取、允许生成或要求处理任何第三方技术资料的，即视为客户已授权 GloryScience 在提供、运行、维护、保护、支持、诊断、适配、测试、改进和优化 Oneasy 服务所必要或合理相关的范围内处理该等资料。

客户应确保其拥有合法取得、披露、提交、上传、配置、授权读取、授权使用及允许 GloryScience 为提供和改进 Oneasy 服务而处理该等资料的充分权利。客户不得提交、上传、配置、授权读取或要求处理其无权披露、无权授权使用、无权复制、无权转授权、无权允许云端处理、无权允许跨境处理，或明确受第三方禁止披露、禁止复制、禁止转授权、禁止平台处理、禁止商业使用限制的第三方技术资料。

为避免疑义，公开发布的行业标准、公开协议规范、公开 RFC、公开 Broadband Forum 技术报告、公开数据模型、公开 MIB、设备厂商公开发布的手册或资料，本身不因 Oneasy 支持、引用、实现或适配而当然构成客户或第三方的保密资料；但其使用仍应受适用的版权声明、许可条件、标准组织规则或公开资料使用条款约束。SNMP walk 结果、CLI/API 输出、配置备份、抓包文件、日志样本、设备运行状态、网络拓扑、性能指标、诊断结果、解析结果或其他由客户设备、客户网络或客户配置生成的数据，应按照其具体内容作为客户数据、客户网络数据、第三方技术资料、网络安全敏感信息或受监管数据处理。

GloryScience 可以基于客户授权资料、公开资料、设备输出结果、SNMP walk 结果、CLI/API 输出、日志、配置、测试结果、兼容性验证和服务运行经验，建立、维护、更新和改进 Oneasy 的协议库、MIB/OID 解析库、字段映射库、命令模板、适配规则、兼容性规则、诊断规则、自动化流程、测试方法、算法、模型、产品功能和其他通用技术成果；但除非取得相关权利人的明确授权，GloryScience 不会向其他客户公开分发客户提交的原始非公开 MIB 文件、私有 OID 表、CLI/API 文档、固件资料、厂商内部文档或其他可识别的第三方保密技术资料。

GloryScience 作为 SaaS 服务提供方，并非设备厂商、系统集成商、渠道伙伴、终端客户、最终用户或其他第三方授权链条的审查机构。除适用法律强制要求或双方另有明确书面约定外，GloryScience 无义务主动核查客户提交、上传、配置、引用、授权读取或要求处理的任何第三方技术资料的权利来源、授权链条、合同限制、保密义务或设备厂商许可条件。

GloryScience 有权在存在合理安全、保密、知识产权、商业秘密、合同限制、设备许可、通信保密、数据保护或合规风险时，对相关资料拒收、隔离、删除、限制访问、限制导出、停止处理，或暂停相关 Agent/VPN/远程接入、API 调用、日志导出、技术支持处理或相关服务功能，且不构成违约。

8.5 Operations, Approval and High-Risk Changes

8.5 操作、审批与高风险变更

1. Oneasy 可提供配置建议、诊断建议、自动化任务、批量任务、脚本执行、工单流程、AI 辅助分析或其他运维辅助能力。
2. 对可能影响生产网络、OLT/ONU 配置、VLAN、QoS、ACL、认证、端口、业务模板、批量开通、批量停机、退网、固件、脚本执行或服务连续性的高风险操作，客户应在执行前进行适当审批、影响评估、维护窗口安排、备份、回滚计划和人员值守。
3. 除双方另有明确书面约定，Oneasy 的建议、自动化能力或远程接入能力不构成 GloryScience 对客户生产网络结果、终端用户服务质量、网络连续性、配置成功率或回滚成功率的保证。
4. 客户保留对其生产网络和相关操作的最终判断、批准和控制权。

8.6 Logging and Audit Trail

8.6 日志与审计追踪

1. GloryScience 将在技术可行范围内通过 Oneasy 服务记录 Agent/VPN 连接状态、远程接入时间、访问来源、访问目标、关键操作、高风险任务和异常事件。
2. 日志保留期限以第六条所述原则、服务配置、Order Form、DPA 或适用法律为准。
3. 客户可在产品功能支持范围内查看、导出或请求与其租户、远程接入或重大安全事件相关的合理日志摘要。
4. GloryScience 有权对日志进行脱敏、汇总、截取或限制，以保护平台安全、其他客户数据、商业秘密、第三方权益或法律合规要求。
5. 如相关日志摘要、日志导出、抓包、配置备份、CLI 输出或诊断文件可能包含第三方技术资料、设备厂商专有资料、客户商业秘密、网络安全敏感信息或受监管数据，GloryScience 可进行脱敏、截取、限制导出、隔离存储、删除或拒绝提供原始内容。

8.7 Emergency Suspension and Security Control

8.7 紧急暂停与安全控制

如 GloryScience 合理认为存在未经授权访问、凭据泄露、恶意操作、异常流量、横向移动风险、客户侧网络入侵、违法使用、监管风险、第三方攻击或可能影响 Oneasy 服务、客户、其他客户、云服务商或第三方安全的情况，GloryScience 可在必要范围内通过 Oneasy 服务暂停、限制、阻断、撤销或拒绝相关 Agent/VPN/远程接入、API 调用、自动化任务或高风险操作，并在合理可行范围内通知客户。

8.8 Customer Responsibility and Limitation

8.8 客户责任与责任限制

客户负责：

1. 自行评估并批准 Oneasy 接入其网络环境；
2. 配置网络隔离、防火墙策略及访问控制；
3. 遵循最小权限原则，仅开放服务所需必要访问权限；
4. 防止 Agent、VPN 或远程接入能力被用于非授权目的；
5. 及时安装 Oneasy 发布的安全更新或采取 Oneasy 建议的缓解措施；

6. 对其内部网络、设备、OLT/ONU、管理网段及相关系统安全负责；
7. 建立适当的内部审批、监控、值守及权限管理机制；
8. 确保其通过 Agent、VPN、Connector、API、支持工单、日志、抓包、配置备份、脚本、诊断文件或服务内配置提交、上传、配置、授权读取、允许生成或要求处理的设备资料、客户网络数据和第三方技术资料具有合法来源、充分授权及必要保密许可；
9. 在必要情况下及时暂停、限制或终止相关远程接入权限。

除因 GloryScience 的故意不当行为或重大过失直接导致外，GloryScience 不对因以下情形导致的损失承担责任：客户侧网络安全缺陷、权限配置不当、网络隔离不足、客户未及时更新远程接入组件、客户未及时撤销凭据、第三方入侵、横向移动攻击、客户内部未授权操作、客户设备或固件缺陷、私有 MIB、私有 OID、未公开接口、厂商专有资料、未经授权第三方技术资料异常、客户误操作、客户未采取合理安全措施导致的风险扩大。

客户理解并同意，客户接受主协议、本安全附录、配置远程接入、提交凭据、上传资料、授权读取设备输出或允许 Oneasy 生成 SNMP walk 结果、CLI/API 输出、配置备份、日志、抓包或诊断结果的行为，构成客户对相关处理活动的授权和指令。GloryScience 有权合理依赖该等授权、指令和操作记录，而无需在每次处理前另行取得单独书面授权或审查客户与第三方之间的授权链条。

---

9. Vulnerability Management

第九条 漏洞管理

GloryScience 将维护商业合理的漏洞管理流程，包括：

1. 安全漏洞识别；
2. 风险评估与优先级分类；
3. 补丁、配置调整、临时缓解措施或风险接受方案制定；
4. 高风险漏洞优先处理；
5. 必要时向受影响客户发布安全通知；
6. 对第三方组件、云服务、开源组件或供应商服务的漏洞进行合理跟踪和风险管理。

除 Order Form、SLA 或专项安全协议另有约定外，GloryScience 将在商业合理范围内按照以下目标处理经确认且影响 Oneasy 服务的安全漏洞：

Severity	Target Remediation or Mitigation
Critical	目标在确认后 7 个日历日内完成修复、缓解或风险隔离
High	目标在确认后 30 个日历日内完成修复、缓解或风险隔离
Medium	目标在确认后 90 个日历日内完成修复、缓解或纳入计划版本
Low	按风险、影响、版本计划和商业合理性处理

上述时限为漏洞管理目标，不构成独立 SLA、服务信用、绝对修复承诺或无条件赔偿承诺。实际处理时间可能受漏洞复杂性、第三方供应商、云服务商、设备厂商、客户环境、兼容性测试、变更窗口、业务连续性风险或安全处置策略影响。

上述漏洞管理目标仅适用于经确认且位于 GloryScience 控制范围内、影响 Oneasy 服务的平台、组件、配置或代码漏洞。客户侧网络、客户设备、OLT/ONU、CPE、固件、私有接口、第三方系统、客户自有云资源或客户配置导致的漏洞或风险，由客户或相关第三方负责处理，除非双方另有书面约定。

客户不得在未经 GloryScience 书面授权的情况下，对 Oneasy 平台、API、生产环境或基础设施进行渗透测试、漏洞扫描、压力测试、红队测试、社会工程测试、拒绝服务测试或其他安全评估。

如客户需要进行安全测试，应提前向 GloryScience 提出书面申请，并在双方确认测试范围、时间、方法、联系人、数据处理、报告共享、修复协调及限制条件后方可实施。

---

10. Backup and Recovery

第十条 备份与恢复

GloryScience 将根据业务需要和行业通行实践实施合理的数据备份策略。

备份措施可能包括：

1. 数据库备份；
2. 配置备份；
3. 日志或关键元数据备份；
4. 灾难恢复所需的备份副本。

除非双方另行签署 SLA、Order Form 或专项协议，任何 RTO、RPO、恢复时间、恢复完整性、业务连续性目标、灾难恢复目标或备份恢复流程说明均不构成具有法律约束力的服务等级承诺。

客户应自行导出、保存或备份其认为重要的数据、配置和报表，尤其是在服务终止、退款、迁移、批量任务、自动化操作、远程运维或重大配置变更前。

---

11. Security Incident Response

第十一条 安全事件响应

GloryScience 将维护合理的安全事件响应流程，包括：

1. 事件识别；
2. 初步评估；
3. 遏制与缓解；
4. 影响范围分析；
5. 客户通知；
6. 修复与复盘。

若 GloryScience 确认发生可能对客户数据、租户数据、个人数据、Oneasy 服务安全或远程接入环境产生重大影响的安全事件，GloryScience 将在法律要求范围内且不无故拖延地通知客户；在合理可行且具备初步确认信息的情况下，通常将在确认重大安全事件后七十二（72）小时内发出初步通知。

如事件性质复杂、仍处于调查阶段、涉及第三方云服务商或网络服务商、存在取证限制、披露可能加剧安全风险，或适用法律另有要求，GloryScience 可在获得进一步信息后分阶段补充通知内容。

通知内容将在 GloryScience 合理掌握信息的范围内包括：

1. 事件性质；
2. 受影响数据类型、系统范围或远程接入环境；
3. 已知或可能产生的影响；
4. 已采取或计划采取的控制、缓解及修复措施；
5. 建议客户采取的风险缓解措施；
6. 后续沟通方式。

GloryScience 可根据事件调查、取证及处置进展，持续补充相关信息。

客户应及时配合 GloryScience 进行事件调查，包括提供必要日志、配置信息、网络信息、联系人支持、客户侧设备信息、客户侧安全工具告警、访问记录及其他合理必要信息。

对于因第三方基础设施服务商、云服务提供商、网络运营商、设备厂商、客户侧环境或不可抗力因素导致的信息延迟、不完整或调查受限情况，GloryScience 将在合理范围内尽商业合理努力提供相关通知与更新。

除非适用法律明确要求或双方另有书面约定，GloryScience 向客户发出的安全事件通知不构成 GloryScience 代表客户向监管机构、终端用户、订户、客户员工或其他第三方作出的通知。客户作为其租户数据、网络、终端用户关系及本地监管义务的责任主体，应自行判断并履行其适用的监管通知、客户通知、订户通知或其他法定义务。

---

12. Personnel Security

第十二条 人员安全

GloryScience 将对接触客户数据或生产系统的人员采取合理管理措施，包括：

1. 保密义务；
2. 权限审批；
3. 离职或岗位变更后的权限回收；
4. 安全意识培训；
5. 对高权限访问进行限制和监督；
6. 根据岗位需要和商业合理性，对涉及高风险系统访问的人员实施更严格的权限管理或操作审计。

GloryScience 可使用员工、关联方人员、承包商或服务提供商支持服务交付，但应确保其在接触客户数据时承担适当保密和安全义务。如员工、关联方人员、承包商或服务提供商在香港以外地区访问客户数据、租户数据、远程接入数据、日志或其他受保护数据，GloryScience 将按照适用 DPA、隐私政策、主协议及适用法律要求实施相应的访问控制、保密义务、跨境传输保障、日志记录和最小必要访问控制。

---

13. Subprocessors and Third-Party Providers

第十三条 子处理者与第三方服务商

GloryScience 可使用第三方服务商支持服务运营，包括：

1. 云基础设施服务商；
2. 支付处理服务商；
3. 日志与监控服务商；
4. 工单和客户支持系统；
5. 邮件和通信服务商；
6. 安全工具服务商；
7. AI 服务提供商（如适用）；
8. 域名、CDN、身份认证、告警通知、分析或其他辅助服务提供商。

GloryScience 将采取商业合理措施，确保相关服务商承担与其服务性质相匹配的数据保护、保密和安全义务。

客户对重要子处理者变更的通知和异议机制，以 DPA、隐私政策或主协议的约定为准。就安全控制事项而言，GloryScience 可根据服务连续性、安全事件处置、供应商停服、法律合规要求或基础设施调整需要更换、暂停或替代相关第三方服务商，并在合理可行范围内通知受影响客户。

---

14. AI Security and Data Use

第十四条 AI 安全与数据使用

Oneasy 的部分功能可能使用 AI、机器学习、大语言模型、RAG、自动化分析、RCA 辅助分析或其他 AI 辅助能力。

除非客户明确书面授权，GloryScience 不会使用可识别的客户数据训练通用人工智能基础模型。

GloryScience 将采取合理措施降低 AI 相关安全风险，包括：

1. 限制 AI 功能访问权限；
2. 避免不必要地向第三方 AI 服务传输可识别客户数据；
3. 对 AI 输出作辅助性、建议性或信息性定位；
4. 要求客户在生产网络执行 AI 建议、配置建议、RCA 建议或自动化任务前进行人工审核；

5. 在商业合理范围内记录 AI 相关关键输入、输出、调用、审批或执行记录，以支持安全审计、问题排查和争议处理。

如客户自行配置、接入或授权使用其自有第三方 LLM API Key、模型服务、云服务、插件或外部 AI 服务，则客户应自行确认相关第三方服务的使用条款、数据处理条款、跨境传输机制、保密义务、安全能力和费用承担。除 GloryScience 对 Oneasy 服务中由其控制的事项承担责任外，GloryScience 不控制该等客户选择的第三方 AI 服务商，也不对该等服务商的模型训练、数据保留、输出质量、合规性、可用性或安全事件承担责任。

客户不得未经人工审核与确认，将 AI 生成内容、RCA 结论、配置建议、脚本建议或自动化建议直接应用于生产网络环境。客户应自行承担因直接执行 AI 输出导致的配置错误、网络中断、业务故障、终端用户投诉或其他损失，除非该损失由 GloryScience 的故意不当行为或重大过失直接导致且适用法律不允许排除相关责任。

如 Oneasy 功能需要调用由 GloryScience 选择的第三方 AI、模型、云模型 API、RAG、向量数据库或类似服务，且该等服务会处理可识别客户数据、租户数据、网络运维数据、远程接入数据或 AI 输入输出数据，则 GloryScience 将按照适用 DPA、隐私政策、子处理者机制及适用法律处理相关数据传输和服务商管理。除非适用服务说明、DPA、Order Form 或客户配置另有约定，GloryScience 将采取商业合理措施，要求该等第三方服务商不得将可识别客户数据用于训练其通用基础模型。

---

15. Customer Security Responsibilities

第十五条 客户安全责任

客户应对其自身环境、账户、网络、设备和使用行为承担安全责任，包括：

1. 管理授权用户；
2. 分配合理权限；
3. 在 Oneasy 支持相关功能时启用 MFA 或其他强认证措施；
4. 保管密码、API Key、Token、VPN 凭据、SNMP community、设备账号、私钥、证书及其他敏感凭据；
5. 配置内部网络隔离、防火墙、ACL、白名单、路由策略和访问控制；
6. 维护 OLT、ONU、服务器、防火墙、交换机、路由器、ACS/NMS、管理网段及其他客户侧设备安全；
7. 定期备份关键业务数据和关键网络配置；
8. 审核配置变更、AI 建议、自动化任务、批量任务、脚本执行和远程运维操作；
9. 确保其拥有访问、管理和操作相关网络设备的合法授权；
10. 确保其通过 Oneasy 上传、提交、配置、引用或授权使用的 MIB、OID、SNMP walk 结果、CLI/API、OMCI、固件资料、设备厂商内部文档、私有接口说明、脚本、抓包、日志样本、配置模板或其他第三方技术资料具有合法来源、充分授权及必要保密许可；
11. 避免通过 Oneasy 上传、处理或存储非法监听、未授权通信截获、违反通信保密法律的数据，或不应提交至 Oneasy 的高敏感数据；
12. 在服务终止、人员变更、凭据泄露、权限变化或安全事件后及时撤销或更换凭据；

13. 指定安全联系人，并在重大安全事件、远程接入异常或高风险操作时提供及时配合。

客户应自行评估配置变更、自动化操作、批量任务、远程运维行为对其网络环境的影响，并对相关操作后果承担责任。客户作为其网络、设备、终端用户关系及本地监管义务的责任主体，应自行满足其适用的电信监管、网络安全、数据保护、通信保密、关键基础设施或类似法律要求。

---

16. Security Documentation and Audit Support

第十六条 安全文档与审计支持

在客户合理要求下，GloryScience 可提供其可公开或可在保密义务下提供的 Oneasy 服务相关安全资料，包括：

1. 安全控制概要或安全白皮书；
2. 技术与组织措施（TOMs）摘要；
3. 子处理者摘要；
4. 数据处理和数据流说明；
5. 安全事件处理流程摘要；
6. 漏洞管理流程摘要；
7. 渗透测试摘要或第三方安全评估摘要（如有且可披露）；
8. 可用的安全认证、报告或第三方评估摘要（如有）；
9. 企业客户安全问卷的合理答复；
10. 其他双方书面约定的企业审计支持材料。

除非双方另行书面约定，GloryScience 无义务接受：

1. 无限制现场审计；
2. 生产环境渗透测试；
3. 未经授权的扫描、压力测试、红队测试或漏洞验证；
4. 访问 GloryScience 或 Oneasy 服务相关内部系统、源代码、模型、提示词、基础设施控制台、其他客户数据或商业秘密；
5. 影响平台安全、稳定性、服务连续性或其他客户权益的审计要求；
6. 过度频繁、不合理、重复性或与客户实际合规需要无关的审计请求。

任何额外审计、专项安全评估、客户定制合规支持、监管配合支持、现场审计、深度问卷、证明材料准备或客户指定格式报告，均应由双方另行书面约定，并可能产生额外费用。

---

17. Data Deletion and Secure Disposal

第十七条 数据删除与安全处置

在客户账户关闭、服务终止、适用数据导出期届满，或客户根据主协议、DPA 或适用法律提出有效删除请求后，GloryScience 将按照主协议、隐私政策、DPA 和适用法律处理客户数据。

通用口径为：

1. 客户通常可在服务终止或账户关闭后的三十（30）日内导出租户数据，除非主协议、Order Form、DPA 或适用法律另有约定；
2. 在服务终止后，GloryScience 将在九十（90）日内启动并完成商业合理的生产环境租户数据删除或匿名化流程；
3. 备份数据、安全日志、审计日志、重大安全事件日志、财务记录、法定留存数据、争议解决所需数据及适用法律允许或要求保留的数据除外；
4. 对于备份系统中的租户数据，GloryScience 通常不会为单一客户从历史备份介质中单独删除数据，但将按照既定备份轮换、覆盖或失效周期使相关数据逐步删除或不可恢复；
5. 被保留的数据将仅在合规、安全、争议解决、备份恢复、审计、财务记录或履行法律义务所必要的范围内处理；
6. GloryScience 可采用删除、匿名化、覆盖、隔离、访问限制或其他商业合理方式进行安全处置。

---

18. Business Continuity

第十八条 业务连续性

GloryScience 将制定并维护商业合理的业务连续性和灾难恢复计划，以降低重大服务中断风险。

除非双方另行签署 SLA、Order Form 或专项协议，业务连续性计划、RTO、RPO、恢复目标、恢复流程说明、备份恢复安排或灾难恢复计划不构成具有法律约束力的服务等级承诺。

对于中大型企业客户、受监管客户或关键业务场景，双方可通过 Enterprise SLA、专项安全附件或 Order Form 另行约定具体可用性、支持响应、RTO、RPO、服务信用、演练或报告义务。任何该等额外承诺均应以书面约定为准。

---

19. Limitations

第十九条 限制声明

本安全附录不构成以下承诺：

1. Oneasy 服务绝对安全；
2. Oneasy 服务永不中断；
3. 数据永不丢失；
4. 安全事件永不发生；
5. GloryScience 或 Oneasy 服务对客户侧网络、设备、配置、凭据、权限、第三方系统或终端用户服务承担安全责任；
6. GloryScience 或 Oneasy 服务已获得未明确声明的任何安全认证；

7. GloryScience 保证客户生产网络、OLT/ONU、终端用户服务、设备兼容性、AI/RCA 结果或自动化任务结果不会发生故障、错误、中断或损失；
8. GloryScience 承担客户作为 ISP、电信运营商、网络运营者、关键基础设施运营者或本地监管义务主体的不可转移法定义务。

GloryScience 在本安全附录项下的责任限制适用《Oneasy SaaS 服务协议》第九条，但适用法律明确禁止限制的责任除外。

---

20. Governing Law and Dispute Resolution

第二十条 法律适用与争议解决

本安全附录的法律适用与争议解决机制，适用《Oneasy SaaS 服务协议》第十二条。

---

21. Order of Precedence

第二十一条 文件优先级

如本安全附录与其他文件存在冲突，就安全控制、安全事件响应、技术与组织安全措施、远程接入安全、Agent/VPN 安全、漏洞管理、日志保留、AI 安全和客户安全责任等事项，以本安全附录为准；如该等事项同时涉及个人数据处理、跨境传输、子处理者、数据主体请求、个人数据泄露通知或数据保护法律义务，则 DPA 中的专门约定优先适用。

如不同文件之间存在冲突，除双方通过 Order Form、SOW、Enterprise SLA 或其他经授权书面文件明确另有约定外，适用以下优先级：

1. Order Form / Subscription Order / SOW / Enterprise SLA；
2. Data Processing Agreement / DPA；
3. Security Addendum；
4. Oneasy SaaS 服务协议；
5. Oneasy 支付退款条款；
6. Oneasy 隐私政策；
7. Oneasy Cookie 政策；
8. Oneasy 网站使用条款。

但对于纯粹支付、退款、账单、自动续费、拒付、逾期付款事项，以支付退款条款为准；对于公开网站访问事项，以网站使用条款为准；对于 Cookie 和追踪技术事项，以 Cookie 政策为准；对于个人数据处理事项，以 DPA 为准；对于安全控制事项，以 Security Addendum 为准，但如安全事项同时涉及个人数据处理、跨境传输、个人数据泄露通知或数据保护法律义务，则 DPA 优先。

Annex A — Security Control Matrix

附件A：安全控制矩阵

Category	Measures	Notes
Security Governance	Security owner/team, internal policies, incident response process, risk review	References to ISO 27001/SOC 2/CSA CCM are control references only unless certified
Access Control	RBAC, least privilege, access approval, access review, production access restriction	Customer manages tenant-side roles and users
Authentication	Password controls, MFA support where available, stronger controls for privileged accounts	Customer should enable MFA for admin users where supported
Encryption in Transit	TLS 1.2+ or equivalent where technically feasible and applicable	Subject to legacy device, integration or protocol constraints
Encryption at Rest	Encryption, isolation, access controls or equivalent safeguards where applicable	Specific encryption architecture may vary by system component
Secret Protection	Credential protection, token/key lifecycle controls, masking in logs where reasonable	Customer controls customer-side device/VPN/API credentials unless agreed otherwise
Third-Party Technical Materials	Submission/configuration/authorized reading/allowed generation constitutes customer authorization; source and authorization boundary; rejection/isolation/deletion/limited access controls where reasonable	Customer may submit authorized MIB/OID/SNMP walk/CLI/API/OMCI/firmware/vendor materials for service purposes, but must not submit unauthorized or restricted materials
Logging	Auth logs, API security logs, admin action logs, Agent/VPN logs, incident logs	Retention periods are governed by Section 6, applicable service configuration, Order Form, DPA, internal retention policy and applicable law.
Network Security	Firewall/security group controls, restricted access, interface protection, abuse monitoring	Does not replace customer-side network security
Infrastructure	Cloud security configuration, environment separation, capacity and availability monitoring	Third-party cloud dependencies apply
Vulnerability Management	Risk-based remediation targets, patches, mitigations, customer notices where necessary	Targets are not independent SLA commitments

Category	Measures	Notes
Incident Response	Detection, containment, customer notification, remediation, updates	72-hour initial notice target for confirmed material incidents where feasible
Backup	Commercially reasonable backup strategy	RTO/RPO only binding if separately agreed
Personnel	Confidentiality obligations, permission controls, training, privileged access oversight	Contractors/providers subject to appropriate obligations
Subprocessors	Vendor selection, contractual safeguards, subprocessor management	Notice/objection governed by DPA/Privacy Policy/main agreement
Remote Access	Agent/VPN scope limitation, customer authorization, logging, revocation, emergency suspension	See Annex C
AI Security	No identifiable customer data training without authorization, advisory outputs, human review	Customer-supplied third-party LLM/API Key risks remain with customer
Audit Support	Security summaries, TOMs, questionnaires, reports where available	No unrestricted audit, pentest, source code or infrastructure access

---

Annex B — Customer Security Checklist

附件B：客户安全责任清单

本清单为客户侧安全责任和建议措施，并不构成 GloryScience 对客户侧环境实施审计、监督、验证或持续监控的义务，除非双方另有书面约定。

客户应至少采取以下措施：

1. 为管理员账户和高权限用户启用 MFA（在 Oneasy 支持相关功能时）；
2. 使用强密码并定期更换；
3. 控制 API Key、Token、SNMP community、设备账号、私钥、证书和 VPN/Agent 凭据；
4. 及时删除不再需要访问权限的用户；
5. 限制 VPN/Agent 可访问的网络范围；
6. 对 OLT/ONU 管理网段进行隔离；
7. 使用防火墙、ACL、白名单、专用账户或跳板机限制访问；
8. 审核 AI 建议、自动化任务、批量配置操作和高风险变更；
9. 在重大配置变更前备份关键配置并准备回滚方案；
10. 定期审查操作日志和远程接入日志；
11. 及时安装 Agent/VPN 安全更新或采取建议的缓解措施；

12. 在人员变动、服务终止或疑似泄露后及时撤销或轮换凭据；
13. 指定安全联系人并配合安全事件调查；
14. 确保接入 Oneasy 的设备、网络和数据具备合法授权；
15. 不提交来源不明、无权披露、无权复制、无权转授权或受第三方保密限制的 MIB、OID、SNMP walk 结果、CLI/API、OMCI、固件资料、设备厂商内部文档、私有接口说明、脚本、抓包、日志样本、配置模板或其他第三方技术资料；
16. 不上传非法监听、未授权通信截获、违反通信保密法律或不应提交至 Oneasy 的高敏感数据。

Annex C — Remote Access Control Schedule

附件C：远程接入控制清单

Control Area	Default Position	Customer Responsibility
Authorization	Remote access requires customer authorization through contract, configuration, SOW, admin console or other agreed method	Confirm legal and operational authority to grant access
Connection Method	Agent/VPN/Connector/API/tunnel as supported and agreed	Approve deployment method and maintain customer-side network controls
Network Scope	Limited to necessary OLT/ONU management interfaces, protocols, ports, accounts and subnets	Restrict network range, ports, routes, ACLs and firewall rules
Prohibited Scope	No access to office networks, HR/finance systems, unrelated internal systems or user traffic content unless expressly agreed	Avoid exposing non-service systems to Oneasy access paths
Credentials	GloryScience protects credentials managed through Oneasy using reasonable controls	Create, rotate, revoke and limit customer-side credentials
Technical Materials	Authorized submission, configuration, authorized reading or allowed generation may be processed for service, adaptation, diagnostics and improvement; GloryScience may reject/isolate/delete/limit export or stop processing unauthorized or high-risk materials	Confirm authority for MIB/OID/SNMP walk/CLI/API/OMCI/firmware/vendor materials and do not submit unauthorized or restricted materials through Agent/VPN/API/support/logs/diagnostics
Privileges	Least privilege and purpose-limited access	Avoid shared admin accounts and unnecessary high privileges

Control Area	Default Position	Customer Responsibility
High-Risk Operations	Customer approval, maintenance window, backup, rollback and audit trail where feasible	Perform impact assessment and retain final operational control
Logging	Connection, access and key operations logged where technically feasible	Review logs and report anomalies promptly
Revocation	Customer may pause, restrict or revoke access by technical controls or notice	Implement revocation and confirm deactivation where needed
Emergency Suspension	GloryScience may suspend or restrict Oneasy access for security, legal, abuse or risk reasons	Cooperate with investigation and remediation
AI / Automation	AI and automation outputs are assistive unless expressly agreed otherwise	Human review before production execution
Incident Cooperation	GloryScience provides reasonable notices and updates for confirmed material incidents	Provide logs, contacts, device information and local investigation support