ADENDO DE SEGURANÇA ONEASY

Versão internacional empresarial aprimorada

Última atualização: 25 de junho de 2026
Data de vigência: 25 de junho de 2026

---

1. FINALIDADE E ESCOPO

Este Adendo de Segurança ("Adendo") complementa o Contrato de Serviços SaaS da Oneasy e descreve as medidas técnicas e organizacionais adotadas pela GloryScience International Limited, por meio da Oneasy SaaS Platform ("Oneasy"), para proteger Dados do Cliente, dados do Tenant, dados operacionais da plataforma e a segurança dos sistemas relacionados.

"GloryScience" significa GloryScience International Limited. "Oneasy" ou "Serviços Oneasy" significa a Oneasy SaaS Platform operada pela GloryScience, suas funções, componentes, APIs, recursos de acesso por Agent/VPN e serviços de suporte. Exceto quando descrever produto ou tecnologia, os direitos, obrigações, limitações e avisos deste Adendo pertencem à GloryScience. A Oneasy não é operadora de telecomunicações, ISP, operadora da rede do Cliente, prestadora de comunicações aos usuários finais nem controladora final da rede de produção do Cliente.

Este Adendo aplica-se à plataforma inteligente de OAM em nuvem, APIs, console administrativo, componentes de acesso remoto, Agent/VPN e suporte fornecidos como SaaS.

Em caso de conflito, este Adendo prevalece quanto a controles de segurança, incidentes, acesso, medidas técnicas e organizacionais, Agent/VPN, acesso remoto, vulnerabilidades, retenção de logs, segurança de IA e responsabilidades de segurança do Cliente. Se a matéria também envolver Tratamento de Dados Pessoais, transferência internacional, Suboperadoras, direitos dos Titulares, notificação de violação ou obrigações legais de proteção de dados, prevalecerá o DPA. As demais matérias permanecem sujeitas ao Contrato Principal.

---

2. GOVERNANÇA DE SEGURANÇA

A GloryScience manterá mecanismos de segurança da informação comercialmente razoáveis, incluindo:

1. responsável ou equipe de segurança;
2. políticas internas, controle de acesso e resposta a incidentes;
3. confidencialidade para empregados, contratados e pessoas autorizadas que acessem Dados do Cliente;
4. avaliações periódicas de risco e melhoria contínua conforme o negócio, ameaças, tecnologia e necessidades razoáveis; e
5. referência, quando razoável, a princípios como ISO 27001, SOC 2 e CSA CCM.

Referências a padrões são apenas referências de controle, salvo certificação formal. Certificação, auditoria ou avaliação futura será comprovada pelo certificado ou relatório efetivo, seu escopo e período de validade.

---

3. HOSPEDAGEM DE DADOS E SEGREGAÇÃO DE TENANTS

1. Por padrão, a hospedagem, o Tratamento e o armazenamento principais da Oneasy localizam-se na região de Singapura do Alibaba Cloud International. A GloryScience poderá usar outras regiões para nós secundários, recuperação de desastres, borda, logs ou acesso de suporte, conforme disponibilidade, segurança, suporte, desempenho, Suboperadoras ou configuração do Cliente.
2. Os Serviços Oneasy usam segregação lógica entre espaços, contas, permissões e dados de diferentes Clientes.
3. A GloryScience adotará medidas razoáveis contra acesso não autorizado entre Tenants.
4. O Cliente administra usuários, funções, permissões e auditoria interna de seu Tenant.
5. Região específica, localização de dados, restrição transfronteiriça, ambiente dedicado, chave exclusiva ou segregação adicional exigem Order Form, SOW, DPA, SLA ou acordo específico e poderão implicar custos adicionais.

---

4. CONTROLE DE ACESSO

A GloryScience aplicará controles comercialmente razoáveis, incluindo RBAC, privilégio mínimo, aprovação e revogação de acesso do pessoal, restrição de acesso à produção, registro de operações privilegiadas, suporte a MFA quando tecnicamente viável, autenticação reforçada para contas internas privilegiadas ou de alto risco, revisões periódicas ou após mudanças e proteção de credenciais, API Keys, tokens e credenciais de VPN/Agent.

O Cliente deverá:

1. administrar adequadamente as contas de administrador e permissões dos Usuários Autorizados;
2. remover prontamente usuários desligados, transferidos ou sem necessidade de acesso;
3. proteger senhas, API Keys, tokens e credenciais de VPN/Agent;
4. habilitar MFA ou autenticação forte para administradores e usuários privilegiados quando suportado; e
5. assumir riscos decorrentes de comprometimento de suas contas, contas compartilhadas, senhas fracas, vazamento de credenciais ou configuração inadequada de permissões.

---

5. CRIPTOGRAFIA E PROTEÇÃO DE DADOS SENSÍVEIS

A GloryScience adotará, conforme práticas do setor, o cenário e padrões comerciais razoáveis:

1. protocolos de transmissão criptografada, preferencialmente TLS 1.2 ou superior, ou segurança equivalente, quando aplicável e tecnicamente viável;
2. criptografia, segregação, controle de acesso ou salvaguarda equivalente para dados em repouso na produção, quando aplicável;
3. hash, criptografia, armazenamento seguro, restrições ou controles equivalentes para senhas, credenciais, chaves e tokens;
4. esforços razoáveis para não expor segredos completos em logs, mensagens de erro, depuração, configurações em texto simples, suporte ou canais inseguros;
5. controles de acesso e auditoria para dados sensíveis; e

6. gestão do ciclo de vida de chaves, certificados, tokens e credenciais, incluindo geração, armazenamento, acesso, rotação, revogação e eliminação.

A GloryScience poderá atualizar medidas conforme tecnologia, riscos, padrões, dependências ou arquitetura, sem reduzir deliberadamente o nível geral de proteção descrito.

O Cliente evitará enviar senhas em texto simples, chaves privadas, informações sensíveis não anonimizadas, interceptação ilegal ou não autorizada e dados de alto risco por campos não designados, suporte comum, mensagens instantâneas ou e-mail inseguro. Salvo acordo escrito, a GloryScience não garante requisitos especializados de determinado setor, país, marco regulatório, certificação de algoritmo ou gestão exclusiva de chaves.

---

6. LOGS E MONITORAMENTO

A GloryScience manterá mecanismos apropriados, conforme práticas razoáveis, necessidades operacionais, conformidade e funções efetivas dos Serviços, para monitorar a plataforma, detectar incidentes, solucionar problemas, analisar acessos anômalos, apoiar auditorias e manter registros de conformidade.

Os logs poderão abranger autenticação, chamadas de API, operações críticas, erros e operação do sistema, incidentes, status e acesso de Agent/VPN ou acesso remoto, alterações de alto risco, tarefas automatizadas ou em lote e operações remotas de OAM.

A GloryScience adotará medidas comercialmente razoáveis contra acesso, adulteração, eliminação anormal ou exportação inadequada, como controle de acesso, integridade, backups, centralização e carimbos de data e hora.

Tipos, granularidade, retenção, acesso e exportação variam conforme versão, implantação, configuração, dados, riscos, lei e Serviços contratados, e seguem o Contrato Principal, DPA, este Adendo, Order Form, configuração ou lei. Salvo obrigação legal ou acordo escrito, a GloryScience não deverá reter logs históricos indefinidamente, fornecer todos os logs brutos, atender padrão forense ou dar acesso além das necessidades razoáveis.

Quando exigido ou razoavelmente necessário, a GloryScience poderá apoiar solicitações relacionadas a incidentes, regulação ou auditoria, com anonimização, agregação, recorte ou restrição para proteger segurança, confidencialidade, outros Clientes, integridade, segredos comerciais e a lei.

Se logs, capturas, backups, saídas de CLI/API ou diagnósticos de Agent/VPN contiverem materiais proprietários de fabricantes, segredos do Cliente, informações sensíveis de cibersegurança ou dados regulados, a GloryScience poderá anonimizá-los, recortá-los, limitar sua exportação, isolá-los ou eliminá-los e restringir acesso, compartilhamento, cópia ou download.

---

7. SEGURANÇA DE REDE E INFRAESTRUTURA

A GloryScience adotará medidas razoáveis, incluindo controle de acesso à rede; firewall, grupos de segurança ou segregação equivalente; configuração segura da nuvem; patches e correções; separação razoável entre produção e não produção; monitoramento de capacidade, disponibilidade e segurança; proteção contra acesso malicioso, tráfego anômalo, força bruta, abuso de privilégios e dos Serviços; e restrição ou monitoramento reforçado de interfaces administrativas, APIs, console, acesso remoto e componentes de alto risco.

Parte da infraestrutura poderá depender de provedores de nuvem, rede, segurança, monitoramento, comunicações ou outros terceiros. A GloryScience selecionará provedores com capacidade apropriada e imporá responsabilidades por contratos, gestão de fornecedores ou mecanismos razoáveis.

---

8. SEGURANÇA DE AGENT, VPN E ACESSO REMOTO

Como a Oneasy pode conectar-se ao ambiente do Cliente por Agent, VPN, Connector, API, túnel, script remoto, ferramenta de OAM ou outro meio, as partes reconhecem a elevada sensibilidade, inclusive o possível acesso a equipamentos, interfaces de OLT/ONU, configurações e ambientes operacionais.

O acesso remoto seguirá, por padrão, autorização do Cliente, limitação de finalidade, privilégio mínimo, exposição mínima da rede, revogabilidade, auditabilidade e controle seguro.

8.1 Estabelecimento e Autorização

1. O acesso será estabelecido por aceitação do Contrato Principal e deste Adendo, configuração dos Serviços, Order Form, plano de implantação, console, ação do administrador, confirmação no produto ou método acordado.
2. Ao aceitar documentos, adicionar dispositivos, configurar credenciais, habilitar Agent, VPN, Connector, API, SNMP, TR-069, TR-369, CLI, Syslog, ACS ou NMS, enviar MIB, OID, resultados de SNMP walk, saídas de CLI/API, backups, logs, capturas, scripts, modelos ou materiais técnicos, ou solicitar suporte, o Cliente autoriza a GloryScience, na medida necessária ou razoavelmente relacionada à prestação, operação, manutenção, proteção, suporte, diagnóstico, adaptação, teste, melhoria e otimização dos Serviços, a acessar, ler, coletar, analisar, armazenar em cache, tratar, exibir, invocar, transmitir ou auxiliar na operação de dispositivos, sistemas, interfaces, contas, credenciais, dados e ambientes de OAM.
3. O Cliente confirmará propriedade, direito operacional ou de gestão, autorização contratual e interna, licença de terceiro ou fabricante, dispensa de confidencialidade, autorização regulatória e aviso ou consentimento do usuário final quanto a OLT, ONU, CPE, ACS, NMS, redes, interfaces, contas, credenciais, dados, logs, configurações, topologias e materiais técnicos.
4. Salvo acordo escrito, a GloryScience não acessará proativamente redes, sistemas, dispositivos ou dados não autorizados e poderá confiar razoavelmente nas declarações, autorizações e registros do Cliente.
5. O Cliente poderá suspender, restringir ou revogar o acesso pelo console, mudança de configuração, política de rede, revogação de credenciais, encerramento da VPN, aviso escrito ou meio razoável. A revogação não afeta a legalidade do Tratamento anterior nem a retenção necessária para segurança, auditoria, backup, disputas, lei ou operação razoável.

8.2 Escopo e Limites de Rede

1. Salvo acordo escrito, o acesso limita-se às interfaces de gestão de OLT/ONU, protocolos, portas, contas, sub-redes, logs, telemetria, configuração e dados operacionais necessários.
2. Não será usado para redes corporativas, finanças, RH, conteúdo do tráfego de usuários finais, sistemas internos não relacionados ou ambientes alheios aos Serviços.
3. O Cliente limitará o escopo por segregação, firewall, grupo de segurança, ACL, lista de permissões, roteamento, jump server, conta dedicada ou outras medidas.
4. Quando viável, Agent ou Connector deverá preferir conexão de saída criptografada iniciada pelo Cliente, VPN aprovada ou método que reduza a superfície exposta.

5. Porta pública, sub-rede fracamente isolada, conta compartilhada, privilégio excessivo ou acesso além da finalidade ficará sob risco do Cliente e poderá exigir confirmação escrita.

8.3 Gestão de Credenciais e Chaves

O Cliente criará, configurará, protegerá, rotacionará e revogará suas contas, SNMP community, API Keys, tokens, credenciais de VPN, contas de dispositivos, chaves privadas, certificados e outros segredos. A GloryScience protegerá comercialmente as credenciais que administrar ou armazenar pelos Serviços e evitará expor segredos completos em texto simples.

O Cliente rotacionará suas contas conforme a política própria e após mudança de pessoal ou autorização, término, suspeita de vazamento ou incidente. Salvo acordo escrito, não fornecerá conta administrativa compartilhada, conta genérica não auditável, privilégio superior à finalidade nem credenciais de produção não relacionadas.

O Cliente não disfarçará, como credencial, configuração, nota, script ou diagnóstico, MIB, OID, SNMP walk, CLI/API, OMCI, firmware, documento interno ou interface privada de origem desconhecida, sem direito de divulgação, sob confidencialidade de terceiro ou proibido para nuvem. Materiais legitimamente fornecidos ou autorizados ficam sujeitos à Seção 8.4.

8.4 Segurança de Materiais Técnicos e de Fabricantes

"Materiais Técnicos de Terceiros" abrangem quaisquer materiais de dispositivo, rede, protocolo, interface ou fabricante fornecidos, exibidos, divulgados, autorizados para leitura ou geração, incluindo MIB, tabelas OID, resultados de SNMP walk, documentação ou saídas de CLI/API, manuais de comandos, interfaces privadas, OMCI, extensões privadas baseadas em TR-069, TR-369 ou TR-181, parâmetros não públicos, modelos privados, documentos ACS/NMS, firmware, modelos de configuração, scripts, capturas, logs, suporte de fabricante, testes, listas de compatibilidade e materiais sujeitos a propriedade intelectual, segredo comercial, contrato ou confidencialidade.

Padrões setoriais, especificações de protocolos, RFCs e relatórios ou modelos TR-069, TR-369 e TR-181 do Broadband Forum disponibilizados publicamente não se tornam materiais confidenciais pelo suporte, referência, implementação, análise ou adaptação da Oneasy. Seu uso continuará sujeito a direitos autorais, licenças e regras aplicáveis.

Extensões privadas, parâmetros e implementações não públicos, documentos internos, MIB/OID privados, CLI/API privadas, saídas de equipamentos, configurações locais, logs, capturas, SNMP walk e diagnósticos poderão constituir Dados do Cliente, dados de rede, materiais técnicos, segredos comerciais ou materiais restritos.

Ao enviar, configurar, autorizar leitura, permitir geração ou solicitar Tratamento desses materiais por Agent, VPN, Connector, API, ticket, logs, capturas, backup, CLI, diagnóstico, script ou modelo, o Cliente autoriza seu Tratamento no limite necessário ou razoavelmente relacionado aos Serviços.

O Cliente assegurará direitos suficientes de obtenção, divulgação, envio, configuração, leitura, uso e Tratamento, e não fornecerá materiais que não possa divulgar, copiar, sublicenciar, tratar na nuvem ou internacionalmente, nem materiais cuja divulgação, cópia, sublicença, Tratamento em plataforma ou uso comercial seja proibido por terceiro.

A GloryScience poderá criar e melhorar bibliotecas de protocolos e MIB/OID, mapeamentos, modelos de comandos, regras de adaptação, compatibilidade e diagnóstico, automações, testes, algoritmos, modelos e funções gerais com base em materiais autorizados ou públicos, saídas, testes e experiência operacional. Sem autorização do titular, não distribuirá a outros Clientes arquivos MIB não públicos originais, tabelas OID

privadas, documentação de CLI/API, firmware, documentos internos ou materiais confidenciais identificáveis enviados pelo Cliente.

A GloryScience não é auditora da cadeia de autorizações entre fabricantes, integradores, canais, clientes finais ou terceiros e, salvo obrigação legal ou acordo escrito, não verificará proativamente origem dos direitos, contratos, confidencialidade ou licenças. Poderá recusar, isolar, eliminar, restringir acesso ou exportação, interromper Tratamento ou suspender Agent/VPN, acesso remoto, API, logs, suporte ou funções por risco razoável de segurança, confidencialidade, propriedade intelectual, licença, sigilo das comunicações, proteção de dados ou conformidade, sem que isso constitua inadimplemento.

8.5 Operações, Aprovação e Alterações de Alto Risco

1. A Oneasy poderá fornecer recomendações de configuração e diagnóstico, tarefas automatizadas ou em lote, execução de scripts, fluxos de tickets, análise assistida por IA e outros recursos auxiliares de OAM.
2. Para operações que possam afetar rede de produção, configurações de OLT/ONU, VLAN, QoS, ACL, autenticação, portas, modelos de serviço, ativações ou desativações em lote, descomissionamento, firmware, scripts ou continuidade, o Cliente realizará aprovação, avaliação de impacto, janela de manutenção, backup, plano de reversão e plantão adequados.
3. Salvo acordo escrito, recomendações, automação ou acesso remoto não garantem resultados da rede de produção, qualidade ao usuário final, continuidade, sucesso de configuração ou reversão.
4. O Cliente conserva o julgamento, a aprovação e o controle finais.

8.6 Logs e Trilha de Auditoria

A GloryScience registrará, quando tecnicamente viável, status de conexão de Agent/VPN, horários, origem, destino, operações críticas, tarefas de alto risco e anomalias. A retenção segue a Seção 6, configuração, Order Form, DPA ou lei. O Cliente poderá consultar, exportar ou solicitar resumos razoáveis quando suportado. A GloryScience poderá anonimizar, agregar, recortar, isolar, eliminar, restringir exportação ou negar conteúdo bruto para proteger plataforma, outros Clientes, segredos, terceiros ou a lei.

8.7 Suspensão Emergencial e Controle de Segurança

Se identificar razoavelmente acesso não autorizado, vazamento de credenciais, operação maliciosa, tráfego anômalo, movimento lateral, intrusão na rede do Cliente, uso ilegal, risco regulatório, ataque de terceiro ou risco à Oneasy, Clientes, nuvem ou terceiros, a GloryScience poderá suspender, restringir, bloquear, revogar ou recusar Agent/VPN, acesso remoto, API, automação ou operação de alto risco na medida necessária e notificará o Cliente quando razoavelmente possível.

8.8 Responsabilidade do Cliente e Limitação

O Cliente deverá avaliar e aprovar o acesso; configurar segregação, firewall e controles; aplicar privilégio mínimo; impedir uso não autorizado; instalar atualizações ou mitigações recomendadas; proteger redes, OLT/ONU, dispositivos e segmentos administrativos; manter aprovação, monitoramento, plantão e permissões; assegurar origem legal, autorização e confidencialidade para dados e materiais técnicos; e suspender ou encerrar prontamente o acesso quando necessário.

Exceto por dolo ou culpa grave diretamente imputável à GloryScience, ela não responderá por perdas decorrentes de falhas na segurança, permissões, segregação, atualização ou revogação pelo Cliente; invasão ou movimento lateral de terceiros; operação interna não autorizada; defeito de dispositivo ou firmware; MIB/OID ou interfaces privadas; materiais técnicos não autorizados; erro do Cliente; ou ampliação do risco pela falta de medidas razoáveis.

A aceitação dos documentos, configuração do acesso, envio de credenciais ou materiais e autorização para leitura ou geração de SNMP walk, CLI/API, backups, logs, capturas ou diagnósticos constitui autorização e instrução. A GloryScience poderá confiar nesses registros sem obter autorização separada a cada Tratamento ou auditar a cadeia de direitos do Cliente.

---

9. GESTÃO DE VULNERABILIDADES

A GloryScience manterá processo comercialmente razoável de identificação, avaliação e priorização, patches, ajustes, mitigação ou aceitação de risco, tratamento prioritário de alto risco, avisos necessários e acompanhamento de componentes de terceiros, nuvem, código aberto e fornecedores.

Salvo disposição em Order Form, SLA ou acordo específico, os objetivos para vulnerabilidades confirmadas que afetem os Serviços são:

1. **Crítica:** correção, mitigação ou isolamento pretendido em até 7 dias corridos após confirmação;
2. **Alta:** em até 30 dias corridos;
3. **Média:** em até 90 dias corridos ou inclusão em versão planejada; e
4. **Baixa:** conforme risco, impacto, planejamento e razoabilidade comercial.

Esses prazos são objetivos de gestão, não SLA, crédito de serviço, promessa absoluta ou indenização incondicional. A duração real poderá depender de complexidade, fornecedores, nuvem, fabricantes, ambiente do Cliente, testes, janelas, continuidade ou estratégia de segurança.

Os objetivos aplicam-se a vulnerabilidades confirmadas em plataforma, componentes, configuração ou código sob controle da GloryScience. Riscos em redes e dispositivos do Cliente, OLT/ONU, CPE, firmware, interfaces privadas, terceiros, nuvem própria ou configuração do Cliente são responsabilidade do Cliente ou terceiro, salvo acordo escrito.

O Cliente não realizará, sem autorização escrita, teste de penetração, varredura, carga, red team, engenharia social, negação de serviço ou avaliação da plataforma, API, produção ou infraestrutura. Testes autorizados exigem acordo prévio sobre escopo, horário, método, contatos, dados, relatório, correção e limitações.

---

10. BACKUP E RECUPERAÇÃO

A GloryScience manterá estratégia razoável, que poderá incluir backups de bancos de dados, configurações, logs ou metadados críticos e cópias para recuperação de desastres.

RTO, RPO, tempo ou integridade de recuperação, continuidade ou procedimentos somente serão compromissos vinculantes quando previstos em SLA, Order Form ou acordo separado. O Cliente exportará e preservará dados, configurações e relatórios importantes, sobretudo antes de término, reembolso, migração, tarefas em lote, automação, OAM remoto ou alteração relevante.

---

11. RESPOSTA A INCIDENTES DE SEGURANÇA

A GloryScience manterá processo razoável de identificação, avaliação inicial, contenção, mitigação, análise de impacto, notificação, correção e revisão.

Ao confirmar incidente com impacto relevante sobre Dados do Cliente, dados do Tenant, Dados Pessoais, segurança dos Serviços ou ambiente de acesso remoto, notificará sem atraso indevido conforme a lei e, quando razoavelmente viável e houver informação preliminar confirmada, normalmente em até setenta e duas (72) horas após a confirmação.

Poderá complementar a notificação por etapas quando o caso for complexo, estiver sob investigação, envolver nuvem ou rede de terceiros, houver restrição forense, a divulgação agravar o risco ou a lei assim exigir. Na medida das informações disponíveis, indicará natureza, dados, sistemas ou acesso afetado, impactos, medidas tomadas ou planejadas, ações recomendadas e comunicação posterior.

O Cliente cooperará prontamente com logs, configurações, informações de rede e dispositivos, contatos, alertas de suas ferramentas e registros de acesso. A GloryScience envidará esforços comercialmente razoáveis diante de atrasos ou limitações causados por infraestrutura, nuvem, rede, fabricantes, ambiente do Cliente ou força maior.

A notificação da GloryScience ao Cliente não substitui aviso do Cliente a autoridades, usuários finais, assinantes, empregados ou terceiros, salvo obrigação legal ou acordo escrito. O Cliente avaliará e cumprirá suas próprias obrigações regulatórias e legais.

---

12. SEGURANÇA DE PESSOAL

A GloryScience aplicará confidencialidade, aprovação e revogação de permissões, treinamento de conscientização, restrição e supervisão de acessos privilegiados e controles reforçados ou auditoria conforme o risco da função.

Poderá usar empregados, afiliados, contratados ou prestadores, impondo obrigações apropriadas. Para acesso fora de Hong Kong, aplicará os controles de acesso, confidencialidade, transferência internacional, logs e acesso mínimo exigidos pelo DPA, Política de Privacidade, Contrato Principal e lei.

---

13. SUBOPERADORAS E PROVEDORES TERCEIROS

A GloryScience poderá usar provedores de infraestrutura em nuvem, processamento de pagamentos, logs e monitoramento, tickets e suporte, e-mail e comunicações, ferramentas de segurança, IA quando aplicável, domínio, CDN, autenticação, alertas, análise ou outros serviços auxiliares. Adotará medidas comercialmente razoáveis para impor proteção de dados, confidencialidade e segurança compatíveis.

Aviso e objeção a Suboperadoras seguem o DPA, Política de Privacidade ou Contrato Principal. Para continuidade, incidente, interrupção de fornecedor, conformidade ou ajuste de infraestrutura, a GloryScience poderá substituir ou suspender provedores e notificará Clientes afetados quando razoavelmente viável.

---

14. SEGURANÇA DE IA E USO DE DADOS

Algumas funções poderão usar IA, machine learning, grandes modelos de linguagem, RAG, análise automatizada, análise auxiliar de RCA ou outros recursos.

Sem autorização escrita, a GloryScience não usará Dados do Cliente identificáveis para treinar modelos gerais de IA. Aplicará medidas razoáveis para restringir acesso a funções de IA, evitar transferências desnecessárias a terceiros, classificar saídas como auxiliares ou informativas, exigir revisão humana antes de executar

recomendações ou automações na produção e, comercialmente, registrar entradas, saídas, chamadas, aprovações ou execuções críticas para auditoria e solução de problemas.

Se o Cliente configurar sua própria API Key de LLM, modelo, nuvem, plugin ou IA externa, ele avaliará os termos, Tratamento de dados, transferências, confidencialidade, segurança e custos. Fora das matérias da Oneasy controladas pela GloryScience, ela não controla o fornecedor escolhido nem responde por treinamento, retenção, qualidade, conformidade, disponibilidade ou incidentes desse terceiro.

O Cliente não aplicará conteúdo, RCA, configuração, script ou automação gerados por IA à produção sem revisão humana. Responderá por erros, interrupções, falhas, reclamações ou perdas dessa execução, salvo dolo ou culpa grave diretamente imputável à GloryScience e responsabilidade não excludente por lei.

Quando a GloryScience selecionar IA, modelo, API de nuvem, RAG, banco vetorial ou serviço semelhante que trate dados identificáveis, administrará a transferência e o fornecedor conforme o DPA, Política de Privacidade, mecanismo de Suboperadoras e lei e, salvo disposição aplicável, exigirá comercialmente que o fornecedor não use dados identificáveis para treinar modelos gerais.

---

15. RESPONSABILIDADES DE SEGURANÇA DO CLIENTE

O Cliente deverá:

1. gerir Usuários Autorizados e permissões;
2. habilitar MFA ou autenticação forte quando suportado;
3. proteger senhas, API Keys, tokens, VPN, SNMP community, contas, chaves e certificados;
4. configurar segregação, firewall, ACL, listas de permissões, rotas e controle de acesso;
5. proteger OLT, ONU, servidores, firewalls, switches, roteadores, ACS/NMS e segmentos administrativos;
6. manter backups de dados e configurações críticas;
7. revisar alterações, recomendações de IA, automações, tarefas em lote, scripts e OAM remoto;
8. assegurar autoridade legal sobre redes e equipamentos;
9. assegurar origem, autorização e confidencialidade de MIB, OID, SNMP walk, CLI/API, OMCI, firmware, documentos de fabricantes, interfaces privadas, scripts, capturas, logs, modelos e materiais técnicos;
10. não enviar interceptação ilegal, comunicação não autorizada, dados contrários ao sigilo ou dados sensíveis inadequados;
11. revogar ou trocar credenciais após término, mudança de pessoal, vazamento, mudança de permissão ou incidente; e
12. indicar contato de segurança e cooperar prontamente em incidentes, anomalias remotas ou alto risco.

O Cliente avaliará e assumirá os efeitos de alterações, automação, tarefas em lote e OAM remoto e cumprirá suas obrigações locais de telecomunicações, cibersegurança, proteção de dados, sigilo e infraestrutura crítica.

---

16. DOCUMENTAÇÃO DE SEGURANÇA E APOIO A AUDITORIA

Mediante solicitação razoável, a GloryScience poderá fornecer materiais divulgáveis ou confidenciais, como visão geral ou white paper, resumo de TOMs e Suboperadoras, fluxos de dados, processos de incidentes e vulnerabilidades, resumos de testes ou avaliações, certificações disponíveis, questionários empresariais e apoio acordado.

Salvo acordo escrito, não aceitará auditoria presencial irrestrita; teste em produção; varredura, carga, red team ou validação não autorizada; acesso a sistemas internos, código-fonte, modelos, prompts, console de infraestrutura, dados de outros Clientes ou segredos; pedido que afete segurança, estabilidade, continuidade ou terceiros; nem pedido excessivo, repetitivo ou sem necessidade real. Apoio adicional, avaliação especial, conformidade personalizada, cooperação regulatória, visita, questionário extenso ou relatório em formato do Cliente exigirá acordo e poderá gerar custos.

---

17. ELIMINAÇÃO E DESCARTE SEGURO

Após fechamento da conta, término, período de exportação ou pedido válido, a GloryScience tratará os Dados do Cliente conforme o Contrato Principal, Política de Privacidade, DPA e lei. Em geral:

1. o Cliente poderá exportar dados do Tenant em até trinta (30) dias, salvo disposição diferente;
2. a GloryScience iniciará e concluirá processo comercialmente razoável de eliminação ou anonimização na produção em até noventa (90) dias após o término;
3. excetuam-se backups, logs de segurança, auditoria e incidentes, registros financeiros, retenção legal, disputas e dados cuja retenção seja permitida ou exigida;
4. dados em backups históricos serão eliminados ou se tornarão irrecuperáveis conforme rotação, sobrescrita ou expiração, sem obrigação de eliminar isoladamente a cópia de um Cliente;
5. dados retidos serão tratados somente para conformidade, segurança, disputas, recuperação, auditoria, finanças ou lei; e
6. a GloryScience poderá eliminar, anonimizar, sobrescrever, isolar, restringir acesso ou usar outro método comercialmente razoável.

---

18. CONTINUIDADE DOS NEGÓCIOS

A GloryScience manterá planos comercialmente razoáveis de continuidade e recuperação de desastres. Sem SLA, Order Form ou acordo específico, planos, RTO, RPO, objetivos, procedimentos ou backups não constituem compromisso vinculante. Clientes empresariais, regulados ou críticos poderão acordar disponibilidade, resposta, RTO, RPO, créditos, exercícios ou relatórios por Enterprise SLA, Adendo ou Order Form.

---

19. LIMITAÇÕES

Este Adendo não promete segurança absoluta, operação ininterrupta, ausência de perda ou incidentes, responsabilidade da GloryScience pela rede, dispositivos, configurações, credenciais, permissões, terceiros ou usuários finais do Cliente, certificação não declarada, ausência de falhas em OLT/ONU, compatibilidade, resultados de IA/RCA ou automação, nem assunção das obrigações legais intransferíveis do Cliente como ISP, operadora de telecomunicações, rede ou infraestrutura crítica.

Aplicam-se as limitações da Seção 9 do Contrato de Serviços SaaS, exceto responsabilidade cuja limitação seja proibida por lei.

---

20. LEI APLICÁVEL E RESOLUÇÃO DE CONTROVÉRSIAS

Aplicam-se a lei e o mecanismo de resolução de controvérsias da Seção 12 do Contrato de Serviços SaaS da Oneasy.

---

21. ORDEM DE PRECEDÊNCIA

Este Adendo prevalece nas matérias de segurança indicadas na Seção 1; o DPA prevalece quando também houver Tratamento de Dados Pessoais, transferência, Suboperadora, direito de Titular, notificação de violação ou obrigação de proteção de dados.

Salvo disposição expressa em instrumento autorizado, a ordem é:

1. Order Form, Subscription Order, SOW ou Enterprise SLA;
2. Data Processing Agreement ou DPA;
3. Security Addendum;
4. Contrato de Serviços SaaS da Oneasy;
5. Termos de Pagamento e Reembolso;
6. Política de Privacidade;
7. Política de Cookies; e
8. Termos de Uso do Site.

Para pagamento, reembolso, faturamento, renovação, chargeback ou atraso, prevalecem os termos de pagamento; para acesso ao site, os Termos de Uso; para cookies, a Política de Cookies; para Dados Pessoais, o DPA; e para controles de segurança, este Adendo, ressalvada a prioridade do DPA nas matérias de proteção de dados.

ANEXO A - MATRIZ DE CONTROLES DE SEGURANÇA

1. **Governança:** responsável ou equipe, políticas, resposta e análise de riscos. ISO 27001, SOC 2 e CSA CCM são referências, salvo certificação.
2. **Controle de acesso:** RBAC, privilégio mínimo, aprovações, revisões e restrição de produção. O Cliente administra funções e usuários do Tenant.

3. **Autenticação:** senhas, MFA quando disponível e controles reforçados para privilégios. O Cliente deve habilitar MFA quando suportado.
4. **Criptografia em trânsito:** TLS 1.2 ou superior, ou equivalente, quando viável, sujeito a limitações de dispositivos, integrações ou protocolos legados.
5. **Proteção em repouso:** criptografia, segregação, acesso ou equivalente conforme o componente.
6. **Segredos:** proteção de credenciais, ciclo de chaves e tokens e mascaramento razoável. O Cliente controla suas credenciais de dispositivo, VPN e API, salvo acordo.
7. **Materiais técnicos de terceiros:** envio, configuração, leitura autorizada ou geração permitida constitui autorização; a GloryScience poderá rejeitar, isolar, eliminar ou limitar materiais de alto risco. O Cliente não enviará MIB/OID, SNMP walk, CLI/API, OMCI, firmware ou materiais de fabricantes sem autorização.
8. **Logs:** autenticação, segurança de API, ações administrativas, Agent/VPN e incidentes. A retenção segue a Seção 6, configuração, Order Form, DPA, política e lei.
9. **Rede:** firewall, grupos de segurança, acesso restrito, proteção de interfaces e monitoramento de abuso. Não substitui a segurança da rede do Cliente.
10. **Infraestrutura:** configuração de nuvem, separação de ambientes e monitoramento, sujeitos a dependências de terceiros.
11. **Vulnerabilidades:** objetivos baseados em risco, patches, mitigação e avisos, sem constituir SLA independente.
12. **Incidentes:** detecção, contenção, notificação, correção e atualizações; objetivo de aviso inicial em 72 horas para incidente relevante confirmado quando viável.
13. **Backup:** estratégia comercialmente razoável; RTO e RPO vinculantes somente se acordados.
14. **Pessoal:** confidencialidade, permissões, treinamento e supervisão; contratados sujeitos a obrigações adequadas.
15. **Suboperadoras:** seleção, contratos e gestão; aviso e objeção conforme DPA, Política de Privacidade ou Contrato Principal.
16. **Acesso remoto:** limites de Agent/VPN, autorização, logs, revogação e suspensão emergencial; ver Anexo C.
17. **IA:** sem treinamento com dados identificáveis sem autorização, saídas consultivas e revisão humana; riscos de LLM/API Key fornecidos pelo Cliente permanecem com ele.
18. **Auditoria:** resumos, TOMs, questionários e relatórios disponíveis; sem auditoria irrestrita, pentest ou acesso a código ou infraestrutura.

ANEXO B - CHECKLIST DE SEGURANÇA DO CLIENTE

Este checklist descreve responsabilidades e recomendações e não impõe à GloryScience auditoria ou monitoramento do ambiente do Cliente, salvo acordo escrito.

O Cliente deverá, no mínimo:

1. habilitar MFA para administradores e usuários privilegiados quando suportado;
2. usar senhas fortes e rotacioná-las;
3. controlar API Keys, tokens, SNMP community, contas, chaves, certificados e VPN/Agent;

4. remover usuários sem necessidade de acesso;
5. limitar a rede acessível por VPN/Agent;
6. segregar segmentos de gestão de OLT/ONU;
7. usar firewall, ACL, listas de permissões, contas dedicadas ou jump server;
8. revisar recomendações de IA, automações, lotes e alto risco;
9. fazer backup e preparar reversão antes de alterações relevantes;
10. revisar logs de operação e acesso remoto;
11. instalar atualizações de Agent/VPN ou mitigações recomendadas;
12. revogar ou rotacionar credenciais após mudanças, término ou suspeita;
13. indicar contato e cooperar em investigações;
14. assegurar autorização legal para equipamentos, redes e dados;
15. não enviar MIB, OID, SNMP walk, CLI/API, OMCI, firmware, documentos internos, interfaces privadas, scripts, capturas, logs, modelos ou materiais de terceiros sem direitos; e
16. não enviar interceptação ilegal, comunicação não autorizada ou dados de alta sensibilidade inadequados.

ANEXO C - QUADRO DE CONTROLE DE ACESSO REMOTO

Autorização

Posição padrão: acesso exige autorização por contrato, configuração, SOW, console ou método acordado.
Responsabilidade do Cliente: confirmar autoridade legal e operacional.

Método de Conexão

Posição padrão: Agent, VPN, Connector, API ou túnel suportado e acordado.
Responsabilidade do Cliente: aprovar a implantação e manter controles de rede.

Escopo de Rede

Posição padrão: interfaces, protocolos, portas, contas e sub-redes de OLT/ONU necessárias.
Responsabilidade do Cliente: restringir rede, portas, rotas, ACLs e firewall.

Escopo Proibido

Posição padrão: sem acesso a rede corporativa, RH, finanças, sistemas não relacionados ou conteúdo de tráfego, salvo acordo expresso.
Responsabilidade do Cliente: não expor sistemas alheios aos Serviços.

Credenciais

Posição padrão: proteção razoável das credenciais geridas na Oneasy.
Responsabilidade do Cliente: criar, rotacionar, revogar e limitar suas credenciais.

Materiais Técnicos

Posição padrão: materiais autorizados poderão ser tratados para Serviços, adaptação, diagnóstico e melhoria; a GloryScience poderá rejeitar, isolar, eliminar, limitar exportação ou interromper materiais não autorizados ou de alto risco.
Responsabilidade do Cliente: confirmar direitos sobre MIB/OID, SNMP walk, CLI/API, OMCI, firmware e materiais de fabricantes e não enviar materiais restritos por Agent, VPN, API, suporte, logs ou diagnósticos.

Privilégios

Posição padrão: privilégio mínimo e acesso limitado à finalidade.
Responsabilidade do Cliente: evitar contas administrativas compartilhadas e privilégios desnecessários.

Operações de Alto Risco

Posição padrão: aprovação, janela, backup, reversão e trilha quando viável.
Responsabilidade do Cliente: avaliar o impacto e manter o controle operacional final.

Logs

Posição padrão: conexão, acesso e operações críticas registrados quando viável.
Responsabilidade do Cliente: revisar e informar anomalias prontamente.

Revogação

Posição padrão: o Cliente pode pausar, restringir ou revogar por controle técnico ou aviso.
Responsabilidade do Cliente: implementar e confirmar a desativação quando necessário.

Suspensão Emergencial

Posição padrão: a GloryScience pode suspender ou restringir por segurança, lei, abuso ou risco.
Responsabilidade do Cliente: cooperar com investigação e correção.

IA e Automação

Posição padrão: saídas são auxiliares, salvo acordo expresso.
Responsabilidade do Cliente: revisão humana antes da execução em produção.

Cooperação em Incidentes

Posição padrão: a GloryScience fornece avisos e atualizações razoáveis sobre incidentes relevantes confirmados.
Responsabilidade do Cliente: fornecer logs, contatos, informações de dispositivos e apoio local à investigação.