Oneasy Security Addendum

Enhanced International Enterprise Edition

Last Updated: June 25, 2026
Effective Date: June 25, 2026

1. Purpose and Scope

This Security Addendum (the "Security Addendum") supplements the Oneasy SaaS Service Agreement and describes the technical and organizational security measures implemented by **GloryScience International Limited** through the Oneasy SaaS Platform ("Oneasy") to protect Customer Data, Tenant Data, Platform Operational Data, and the security of related systems.

For the avoidance of doubt, in this Security Addendum, "GloryScience" means GloryScience International Limited; and "Oneasy" or the "Oneasy Services" means the Oneasy SaaS Platform, related features, components, APIs, Agent/VPN access capabilities, and support services provided and operated by GloryScience. Except where used to describe a product, platform, feature, or technical component, all rights, obligations, limitations of liability, and Customer-notification obligations under this Security Addendum are held or undertaken by GloryScience. Oneasy shall not be interpreted as a telecommunications carrier, ISP, operator of the Customer's network, provider of communications services to the Customer's end users, or the ultimate controller of the Customer's production network.

This Security Addendum applies to the cloud-based intelligent operations and maintenance platform, APIs, administrative console, remote-access components, Agent/VPN access capabilities, and related support services provided to Customers by Oneasy through the SaaS model.

If this Security Addendum conflicts with the Master Agreement, this Security Addendum shall prevail with respect to security controls, security-incident response, access control, technical and organizational security measures, Agent/VPN/remote-access security, vulnerability management, log retention, AI security, and Customer security responsibilities. If any such matter also involves Personal Data Processing, cross-border transfers, Subprocessors, Data Subject Requests, Personal Data Breach notification, or obligations under Data Protection Laws, the specific provisions of the DPA shall prevail. All other matters remain governed by the Master Agreement.

2. Security Governance

GloryScience will establish and maintain a commercially reasonable information-security management framework, including:

1. designating a person responsible for security management or a security management team;
2. establishing internal security-management policies, access-control procedures, and incident-response procedures;
3. imposing confidentiality obligations on employees, contractors, or other authorized personnel who access Customer Data;
4. periodically assessing platform security risks and continuously improving security controls in light of business development, changes in threats, technical conditions, and reasonable Customer requirements; and
5. referring, within reasonable limits, to generally accepted industry security principles such as ISO 27001, SOC 2, and the CSA CCM.

Unless Oneasy has obtained a formal certification, references in this Security Addendum to ISO 27001, SOC 2, the CSA CCM, or any other standard indicate only security-control references and do not constitute a representation that Oneasy has passed or obtained any such certification, audit, or assurance. If Oneasy later obtains any relevant certification, report, or third-party assessment, the actual certificate, audit report, scope of applicability, and validity period shall control.

3. Data Hosting and Segregation

1. By default, Oneasy's primary cloud hosting, primary data processing, and primary storage region is the Alibaba Cloud International Singapore region. GloryScience may establish secondary nodes, disaster-recovery nodes,

edge nodes, logging nodes, or support-access nodes in other regions for service availability, disaster recovery, security protection, technical support, performance optimization, Subprocessor services, or Customer configuration.

2. GloryScience will use logical-segregation mechanisms through the Oneasy Services to separate the tenant spaces, accounts, permissions, and data of different Customers.
3. GloryScience will take reasonable measures to prevent unauthorized cross-tenant access.
4. The Customer is responsible for user management, role assignment, permission configuration, and internal access audits within its Tenant.
5. If the Customer requires a specific data region, data localization, cross-border transfer restrictions, a dedicated environment, dedicated keys, or additional segregation measures, the parties shall agree separately through an Order Form, SOW, DPA, SLA, or specific agreement, and additional fees may apply.

4. Access Control

GloryScience will implement commercially reasonable access-control measures through the Oneasy Services, including:

1. role-based access control (RBAC);
2. the principle of least privilege;
3. mechanisms for approving and revoking employee access rights;
4. restrictions on access to production systems;
5. logging of privileged operations;
6. support for multi-factor authentication (MFA) where technically feasible, with stronger authentication controls applied to internal privileged accounts, production-environment access accounts, or other high-risk accounts;
7. periodic review of internal access rights, as well as review following personnel changes, changes in responsibilities, permission anomalies, or security incidents; and
8. reasonable protection measures for access credentials, API Keys, access tokens, VPN/Agent credentials, and other sensitive authentication information.

The Customer is responsible for:

1. properly managing its administrator accounts;
2. assigning appropriate permissions to Authorized Users;
3. promptly removing users who have left employment, changed roles, or no longer require access;
4. properly safeguarding passwords, API Keys, access tokens, VPN/Agent credentials, and other sensitive credentials;
5. enabling MFA or other strong authentication measures for administrator accounts and privileged users where Oneasy supports the relevant functionality; and
6. assuming responsibility for risks arising from compromise of the Customer's own accounts, shared accounts, weak passwords, credential leakage, or improper permission configuration.

5. Encryption and Sensitive Data Protection

GloryScience will implement appropriate technical and organizational measures through the Oneasy Services to protect data security in accordance with generally accepted industry security practices, the applicable service scenario, and reasonable commercial standards, including, without limitation:

1. using generally accepted encrypted transmission protocols for data in transit. Where technically feasible and applicable, GloryScience will prioritize TLS 1.2 or higher, or a protocol providing an equivalent level of security, through the Oneasy Services;
2. applying reasonable encryption, segregation, access controls, or equivalent safeguards to data at rest in production environments where applicable;
3. applying reasonable protection measures to passwords, access credentials, keys, tokens, and other sensitive authentication information, including hashing, encryption, secure storage, access restrictions, or other equivalent security measures;
4. using reasonable efforts to avoid exposing complete sensitive information in logs, error messages, debugging output, plain-text configurations, Customer-support communications, or insecure channels;
5. implementing appropriate access controls, permission restrictions, and audit records for access to sensitive data in accordance with reasonable security practices; and
6. implementing, to the extent commercially reasonable, lifecycle management for keys, certificates, tokens, and sensitive credentials, including generation, storage, access, rotation, revocation, and deletion.

GloryScience may update or adjust the relevant security measures in response to technological developments, security risks, updates to industry standards, changes in third-party dependencies, or service-architecture adjustments, but will not intentionally reduce the overall level of security protection described in this Security Addendum.

The Customer should avoid submitting plaintext passwords, private keys, unredacted sensitive personal information, unlawful surveillance data, unauthorized intercepted communications data, or other high-risk sensitive data through non-designated fields, ordinary support channels, instant messaging, insecure email, or other insecure means.

Unless otherwise agreed by the parties in writing, GloryScience does not undertake to satisfy specialized requirements under any particular industry, country, regulatory framework, encryption-algorithm certification, or dedicated key-management scheme.

6. Logging and Monitoring

GloryScience will maintain appropriate logging and monitoring mechanisms based on reasonable security practices, service-operational needs, compliance requirements, and the actual functionality of the Oneasy Services, for purposes including platform-operation monitoring, security-incident detection, troubleshooting, anomalous-access analysis, audit support, and compliance records.

Relevant logs may include login and authentication records, API-call records, key-operation records, system-error and runtime logs, security-incident-related logs, Agent/VPN or remote-access connection status and access records, and records relating to high-risk configuration changes, automated tasks, batch tasks, or remote operations and maintenance activities.

GloryScience will take appropriate measures, to the extent commercially reasonable, to reduce the risk of unauthorized access to, tampering with, abnormal deletion of, or improper export of logs. Such measures may include access controls, permission restrictions, integrity protection, backups, centralized log management, timestamping, or other equivalent controls.

The specific types of logs, level of detail, retention periods, methods of access, and export capabilities may vary depending on the service version, deployment model, system configuration, data type, security risk, legal requirements, and scope of Services ordered by the Customer, and shall be governed by the Master Agreement, DPA, Security Addendum, Order Form, system configuration, or Applicable Law.

Unless otherwise mandatorily required by Applicable Law or agreed by the parties in writing, GloryScience is not obligated to retain historical logs for an extended period, provide complete raw system logs, meet forensic-evidence standards, or provide log access beyond what is reasonably required for operations, security support, and compliance.

Where required by Applicable Law or reasonably necessary for compliance, GloryScience may, within reasonable limits, assist the Customer with log-support requests relating to security incidents, regulatory requirements, or audits. GloryScience may reasonably redact, aggregate, excerpt, or restrict access to relevant log content based on security, confidentiality, the rights and interests of other Customers, system integrity, trade secrets, or legal restrictions.

If logs, packet-capture files, configuration backups, CLI outputs, API responses, Agent/VPN diagnostic files, or other troubleshooting materials may contain proprietary materials of third-party equipment vendors, Customer trade secrets, cybersecurity-sensitive information, or Regulated Data, GloryScience may, to the extent commercially reasonable, redact, excerpt, restrict export of, isolate, store, or delete the relevant content, and may restrict access to, sharing, copying, or downloading of such content based on security, confidentiality, third-party rights, intellectual property, trade secrets, or Applicable Law.

7. Network and Infrastructure Security

GloryScience will implement reasonable network and infrastructure safeguards, including:

1. network access controls;
2. firewalls, security groups, or equivalent segregation measures;
3. secure configuration of cloud infrastructure;
4. security-patch and vulnerability-remediation processes;
5. reasonable segregation between production and non-production environments;
6. capacity, availability, and security monitoring of critical components;
7. reasonable technical measures to protect against malicious access, anomalous traffic, brute-force attacks, privilege abuse, and service abuse; and
8. access restrictions or enhanced monitoring, where applicable, for administrative interfaces, APIs, backend entry points, remote-access entry points, and high-risk components.

Certain infrastructure supporting the Oneasy Services may depend on third-party cloud service providers, network service providers, security service providers, monitoring service providers, communications service providers, or other third-party providers. GloryScience will take commercially reasonable measures to select service providers with appropriate security capabilities and will impose security responsibilities on them through contracts, vendor management, or other reasonable mechanisms.

8. Agent / VPN / Remote Access Security

Because Oneasy may connect to the Customer's network environment through an Agent, VPN, Connector, API, tunnel, remote script, operations and maintenance tool, or another remote-access method, the parties acknowledge that this scenario is highly security-sensitive and may involve access to the Customer's network equipment, OLT/ONU management interfaces, configuration systems, or operations and maintenance environment.

Oneasy's remote-access capabilities shall, by default, follow the principles of Customer authorization, purpose limitation, least privilege, minimum network exposure, revocability, auditability, and secure controllability.

8.1 Access Establishment and Authorization

1. Remote access shall be established on the basis of the Customer's acceptance of the Master Agreement and this Security Addendum, service configuration, an Order Form, an implementation plan, backend configuration, administrator actions, in-product confirmation, or another method accepted by both parties.
2. If the Customer clicks to accept the Master Agreement or this Security Addendum, adds devices, configures credentials, enables Agent / VPN / Connector / API / SNMP / TR-069 / TR-369 / CLI / Syslog / ACS / NMS interfaces, uploads or submits MIBs, OIDs, SNMP walk results, CLI/API outputs, configuration backups, logs, packet-capture files, scripts, templates, equipment materials, vendor materials, or other Third-Party Technical Materials, or otherwise requests that GloryScience provide relevant support, the Customer will be deemed to have authorized GloryScience, to the extent necessary or reasonably related to providing, operating, maintaining, protecting, supporting, diagnosing, adapting, testing, improving, and optimizing the Oneasy Services, to access, read, collect, parse, cache, process, display, analyze, invoke, issue instructions to, or assist in operating the relevant devices, systems, interfaces, accounts, credentials, data, and operations and maintenance environment.
3. The Customer shall confirm that it possesses sufficient ownership rights, operational rights, management rights, authorized operations and maintenance rights, contractual authorizations, internal approvals, third-party permissions, equipment-vendor permissions, confidentiality waivers, regulatory permissions, end-user notices or consents, or other lawful bases with respect to the relevant OLTs, ONUs, CPEs, ACSs, NMSs, networks, interfaces, accounts, credentials, data, logs, configurations, topologies, Customer Network Data, and Third-Party Technical Materials.
4. Unless otherwise agreed by the parties in writing, GloryScience will not proactively access through the Oneasy Services any network, system, device, or data that the Customer has not authorized. GloryScience may reasonably rely on the representations, warranties, authorizations, and operational records made or provided by the Customer in the Master Agreement, this Security Addendum, service configuration, upload records, authorized-reading records, administrator actions, in-product confirmations, support tickets, or other in-service instructions.
5. The Customer may suspend, restrict, or revoke remote access through the administrative console, configuration changes, network policies, credential revocation, VPN shutdown, written notice, or other reasonable means. Such revocation will not affect the lawfulness of Processing activities performed before revocation in accordance with the Customer's authorization, nor will it affect GloryScience's retention of necessary records for security, audit, backup, preservation of evidence in disputes, legal obligations, or reasonable operational needs.

8.2 Access Scope and Network Boundary

1. Unless otherwise agreed by the parties in writing, remote access is limited to the OLT/ONU management interfaces, protocols, ports, accounts, network segments, logs, telemetry, configurations, or operations and maintenance data necessary to provide the Services.
2. Remote access shall not be used to access the Customer's office network, finance systems, human-resources systems, end-user service-traffic content, internal systems for non-service purposes, or environments unrelated to the purposes of the Oneasy Services.
3. The Customer shall limit the scope accessible by the Agent/VPN through network segregation, firewalls, security groups, ACLs, allowlists, routing policies, bastion hosts, dedicated accounts, or other measures.
4. Where technically feasible and applicable to the deployment model, an Agent or Connector should preferably use a Customer-initiated encrypted outbound connection, a Customer-approved VPN tunnel, or another access method that reduces the exposed attack surface.
5. If the Customer requires publicly exposed ports, weakly segregated network segments, shared accounts, excessively privileged accounts, or access beyond the purposes of the Services, the Customer shall bear the corresponding risks, and the parties may be required to confirm such arrangements separately in writing.

8.3 Credential and Key Management

1. The Customer is responsible for creating, configuring, safeguarding, rotating, and revoking Customer-side accounts, SNMP communities, API Keys, Tokens, VPN credentials, device accounts, private keys, certificates, or other sensitive credentials that it provides to Oneasy or configures in Oneasy.
2. GloryScience will, to the extent commercially reasonable, protect remote-access credentials managed or stored by GloryScience through the Oneasy Services and avoid exposing complete sensitive credentials in ordinary plaintext form.

3. For device accounts, network accounts, VPN accounts, or local-system accounts controlled by the Customer, the Customer shall rotate them periodically in accordance with its own security policies and shall promptly revoke or replace them following personnel changes, changes in authorization scope, termination of Services, suspected leakage, or a security incident.
4. Unless otherwise agreed by the parties in writing, the Customer shall not provide Oneasy with shared administrator accounts, generic accounts that cannot be audited, privileged accounts exceeding the purposes of the Services, or credentials for production systems unrelated to the Services.
5. The Customer shall not disguise MIBs, OIDs, SNMP walk results, CLI/API materials, OMCI materials, firmware materials, equipment-vendor internal documents, private-interface descriptions, or other Third-Party Technical Materials that are of unknown origin, that the Customer has no right to disclose or authorize for use, that are subject to third-party confidentiality restrictions, or that are expressly prohibited from cloud Processing, as credentials, configuration parameters, support materials, notes, scripts, or diagnostic files and submit them to Oneasy. Where the Customer has the right to provide such materials or authorize their reading, the Customer's submission, configuration, uploading, authorization for reading, or permission for generation of such materials through the Oneasy Services shall be governed by Section 8.4.

8.4 Technical Materials and Vendor Materials Security

For purposes of this Security Addendum, **Third-Party Technical Materials** means any equipment, network, protocol, interface, or vendor materials provided, uploaded, transmitted, displayed, disclosed, referenced, authorized for reading, permitted to be generated, or requested for use by a Customer, channel partner, equipment vendor, agent, system integrator, supplier, or other third party to or through GloryScience or Oneasy, including, without limitation, MIB files, OID tables, SNMP walk results, CLI/API documentation or outputs, command manuals, private-interface descriptions, OMCI materials, vendor-specific extensions based on TR-069 / TR-369 / TR-181 or other public standards, non-public parameters, private data models, ACS/NMS interface documentation, firmware descriptions, configuration templates, scripts, packet-capture files, log samples, vendor-support materials, equipment test reports, compatibility lists, supplier-confidential materials, or other materials that may be protected by intellectual property rights, trade secrets, contractual restrictions, or confidentiality obligations.

For the avoidance of doubt, publicly released industry standards, public protocol specifications, public RFCs, TR-069, TR-369, and TR-181 technical reports or data models publicly released by the Broadband Forum, and other lawfully public materials do not, merely because Oneasy supports, references, implements, parses, or adapts them, automatically constitute confidential third-party materials or protected Third-Party Technical Materials. Use of such public materials remains subject to any applicable copyright notices, license terms, conditions of use, or rules of the relevant standards organization.

Vendor-specific extensions, non-public parameters, non-public implementation descriptions, vendor internal documents, private MIBs/OIDs, private CLI/API materials, device outputs, Customer-site configurations, logs, packet captures, SNMP walk results, diagnostic results, or other non-public materials created by vendors, Customers, system integrators, or other third parties based on public standards may nevertheless constitute Customer Data, Customer Network Data, Third-Party Technical Materials, trade secrets, Confidential Information, or materials subject to contractual restrictions.

If the Customer submits, uploads, configures, authorizes the reading of, permits the generation of, or requests the Processing of any Third-Party Technical Materials through an Agent, VPN, Connector, API, support ticket, log upload, packet-capture file, configuration backup, CLI output, diagnostic file, script, configuration template, or other means, the Customer will be deemed to have authorized GloryScience to process such materials to the extent necessary or reasonably related to providing, operating, maintaining, protecting, supporting, diagnosing, adapting, testing, improving, and optimizing the Oneasy Services.

The Customer shall ensure that it possesses sufficient rights to lawfully obtain, disclose, submit, upload, configure, authorize the reading of, authorize the use of, and permit GloryScience to process such materials for the provision and improvement of the Oneasy Services. The Customer shall not submit, upload, configure, authorize the reading of, or request the Processing of Third-Party Technical Materials that it has no right to disclose, authorize for use, copy, sublicense, permit for cloud Processing, or permit for cross-border Processing, or that are expressly subject to third-party restrictions prohibiting disclosure, copying, sublicensing, platform Processing, or commercial use.

For the avoidance of doubt, publicly released industry standards, public protocol specifications, public RFCs, public Broadband Forum technical reports, public data models, public MIBs, and manuals or materials publicly released by equipment vendors do not, merely because Oneasy supports, references, implements, or adapts them, automatically constitute confidential materials of a Customer or third party; however, their use remains subject to applicable copyright notices, license conditions, standards-organization rules, or terms governing the use of public materials. SNMP walk results, CLI/API outputs, configuration backups, packet-capture files, log samples, device-operating status, network topology, performance metrics, diagnostic results, parsing results, or other data generated by Customer devices, Customer networks, or Customer configurations shall, depending on their specific content, be processed as Customer Data, Customer Network Data, Third-Party Technical Materials, cybersecurity-sensitive information, or Regulated Data.

GloryScience may, based on materials authorized by the Customer, public materials, device outputs, SNMP walk results, CLI/API outputs, logs, configurations, test results, compatibility validation, and experience operating the Services, establish, maintain, update, and improve Oneasy's protocol libraries, MIB/OID parsing libraries, field-

mapping libraries, command templates, adaptation rules, compatibility rules, diagnostic rules, automated processes, testing methods, algorithms, models, product features, and other general technical results. However, unless expressly authorized by the relevant rights holder, GloryScience will not publicly distribute to other Customers the original non-public MIB files, private OID tables, CLI/API documentation, firmware materials, vendor internal documents, or other identifiable confidential third-party technical materials submitted by the Customer.

As a SaaS service provider, GloryScience is not the entity responsible for reviewing the chain of authorization among equipment vendors, system integrators, channel partners, end customers, end users, or other third parties. Unless mandatorily required by Applicable Law or expressly agreed by the parties in writing, GloryScience is not obligated to proactively verify the source of rights, chain of authorization, contractual restrictions, confidentiality obligations, or equipment-vendor licensing conditions applicable to any Third-Party Technical Materials submitted, uploaded, configured, referenced, authorized for reading, or requested for Processing by the Customer.

Where reasonable security, confidentiality, intellectual-property, trade-secret, contractual-restriction, equipment-license, communications-secrecy, data-protection, or compliance risks exist, GloryScience may reject, isolate, delete, restrict access to, restrict export of, or cease Processing the relevant materials, or suspend related Agent/VPN/remote access, API calls, log exports, technical-support Processing, or related service functionality, without constituting a breach.

8.5 Operations, Approval and High-Risk Changes

1. Oneasy may provide configuration recommendations, diagnostic recommendations, automated tasks, batch tasks, script execution, ticket workflows, AI-assisted analysis, or other operations and maintenance assistance capabilities.
2. For high-risk operations that may affect the production network, OLT/ONU configurations, VLANs, QoS, ACLs, authentication, ports, service templates, batch activation, batch suspension, decommissioning, firmware, script execution, or service continuity, the Customer shall conduct appropriate approval, impact assessment, maintenance-window planning, backup, rollback planning, and personnel-on-duty arrangements before execution.
3. Unless otherwise expressly agreed by the parties in writing, Oneasy recommendations, automation capabilities, or remote-access capabilities do not constitute a guarantee by GloryScience regarding outcomes in the Customer's production network, quality of service for end users, network continuity, configuration-success rates, or rollback-success rates.
4. The Customer retains final judgment, approval, and control over its production network and related operations.

8.6 Logging and Audit Trail

1. GloryScience will, where technically feasible, record through the Oneasy Services the Agent/VPN connection status, remote-access time, access source, access target, key operations, high-risk tasks, and anomalous events.
2. Log-retention periods shall be governed by the principles in Section 6, service configuration, an Order Form, the DPA, or Applicable Law.
3. To the extent supported by product functionality, the Customer may view, export, or request reasonable log summaries relating to its Tenant, remote access, or a material security incident.
4. GloryScience may redact, aggregate, excerpt, or restrict logs to protect platform security, other Customers' data, trade secrets, third-party rights, or legal-compliance requirements.
5. If relevant log summaries, log exports, packet captures, configuration backups, CLI outputs, or diagnostic files may contain Third-Party Technical Materials, equipment-vendor proprietary materials, Customer trade secrets, cybersecurity-sensitive information, or Regulated Data, GloryScience may redact, excerpt, restrict export of, isolate, store, delete, or decline to provide the original content.

8.7 Emergency Suspension and Security Control

If GloryScience reasonably believes that there is unauthorized access, credential leakage, malicious operation, anomalous traffic, a risk of lateral movement, an intrusion into the Customer-side network, unlawful use, regulatory risk, a third-party attack, or another circumstance that may affect the security of the Oneasy Services, the Customer, other Customers, a cloud service provider, or a third party, GloryScience may, to the extent necessary, suspend, restrict, block, revoke, or refuse related Agent/VPN/remote access, API calls, automated tasks, or high-risk operations through the Oneasy Services, and will notify the Customer where reasonably feasible.

8.8 Customer Responsibility and Limitation

The Customer is responsible for:

1. independently assessing and approving Oneasy's access to its network environment;
2. configuring network segregation, firewall policies, and access controls;
3. following the principle of least privilege and opening only the access permissions necessary for the Services;
4. preventing Agent, VPN, or remote-access capabilities from being used for unauthorized purposes;
5. promptly installing security updates released by Oneasy or implementing mitigation measures recommended by Oneasy;

6. the security of its internal networks, equipment, OLTs/ONUs, management network segments, and related systems;
7. establishing appropriate internal approval, monitoring, personnel-on-duty, and permission-management mechanisms;
8. ensuring that equipment materials, Customer Network Data, and Third-Party Technical Materials submitted, uploaded, configured, authorized for reading, permitted to be generated, or requested for Processing through an Agent, VPN, Connector, API, support ticket, log, packet capture, configuration backup, script, diagnostic file, or in-service configuration have a lawful source, sufficient authorization, and the necessary confidentiality permissions; and
9. promptly suspending, restricting, or terminating the relevant remote-access permissions where necessary.

Except where directly caused by GloryScience's willful misconduct or gross negligence, GloryScience shall not be liable for losses caused by Customer-side network-security deficiencies, improper permission configuration, insufficient network segregation, the Customer's failure to update remote-access components in a timely manner, the Customer's failure to revoke credentials in a timely manner, third-party intrusion, lateral-movement attacks, unauthorized internal Customer operations, defects in Customer equipment or firmware, private MIBs, private OIDs, non-public interfaces, vendor-proprietary materials, anomalies involving unauthorized Third-Party Technical Materials, Customer operational errors, or the expansion of risk caused by the Customer's failure to take reasonable security measures.

The Customer understands and agrees that its acceptance of the Master Agreement and this Security Addendum, configuration of remote access, submission of credentials, uploading of materials, authorization to read device outputs, or permission for Oneasy to generate SNMP walk results, CLI/API outputs, configuration backups, logs, packet captures, or diagnostic results constitutes the Customer's authorization and instruction for the relevant Processing activities. GloryScience may reasonably rely on such authorizations, instructions, and operational records without separately obtaining written authorization before each Processing activity or reviewing the chain of authorization between the Customer and any third party.

9. Vulnerability Management

GloryScience will maintain a commercially reasonable vulnerability-management process, including:

1. identification of security vulnerabilities;
2. risk assessment and priority classification;
3. development of patches, configuration adjustments, temporary mitigations, or risk-acceptance plans;
4. prioritized handling of high-risk vulnerabilities;
5. issuance of security notices to affected Customers where necessary; and
6. reasonable tracking and risk management of vulnerabilities in third-party components, cloud services, open-source components, or vendor services.

Unless otherwise agreed in an Order Form, SLA, or specific security agreement, GloryScience will, to the extent commercially reasonable, address confirmed security vulnerabilities affecting the Oneasy Services according to the following targets:

Severity	Target Remediation or Mitigation
Critical	Target completion of remediation, mitigation, or risk isolation within 7 calendar days after confirmation
High	Target completion of remediation, mitigation, or risk isolation within 30 calendar days after confirmation
Medium	Target completion of remediation, mitigation, or inclusion in a planned release within 90 calendar days after confirmation
Low	Handled according to risk, impact, release plans, and commercial reasonableness

The foregoing periods are vulnerability-management targets and do not constitute an independent SLA, service credits, an absolute remediation commitment, or an unconditional compensation commitment. Actual handling time may be affected by vulnerability complexity, third-party vendors, cloud service providers, equipment vendors, the Customer environment, compatibility testing, change windows, business-continuity risks, or security-response strategy.

The foregoing vulnerability-management targets apply only to confirmed vulnerabilities affecting the Oneasy Services that are within GloryScience's control and relate to the platform, components, configurations, or code. Vulnerabilities or risks arising from Customer-side networks, Customer equipment, OLTs/ONUs, CPEs, firmware, private interfaces, third-party systems, Customer-owned cloud resources, or Customer configurations are the responsibility of the Customer or the relevant third party, unless otherwise agreed by the parties in writing.

The Customer shall not conduct penetration testing, vulnerability scanning, stress testing, red-team testing, social-engineering testing, denial-of-service testing, or any other security assessment of the Oneasy Platform, APIs, production environment, or infrastructure without GloryScience's written authorization.

If the Customer needs to conduct security testing, it shall submit a written request to GloryScience in advance and may proceed only after the parties have confirmed the testing scope, timing, methods, contacts, data handling, report sharing, remediation coordination, and limitations.

10. Backup and Recovery

GloryScience will implement a reasonable data-backup strategy based on business needs and generally accepted industry practices.

Backup measures may include:

1. database backups;
2. configuration backups;
3. backups of logs or critical metadata; and
4. backup copies required for disaster recovery.

Unless the parties separately sign an SLA, Order Form, or specific agreement, any description of RTO, RPO, recovery time, recovery completeness, business-continuity objectives, disaster-recovery objectives, or backup-and-recovery procedures does not constitute a legally binding service-level commitment.

The Customer shall independently export, retain, or back up any data, configurations, and reports that it considers important, particularly before service termination, a refund, migration, batch tasks, automated operations, remote operations and maintenance, or material configuration changes.

11. Security Incident Response

GloryScience will maintain a reasonable security-incident response process, including:

1. incident identification;
2. preliminary assessment;
3. containment and mitigation;
4. impact-scope analysis;
5. Customer notification; and
6. remediation and post-incident review.

If GloryScience confirms a security incident that may materially affect Customer Data, Tenant Data, Personal Data, the security of the Oneasy Services, or the remote-access environment, GloryScience will notify the Customer within the scope required by law and without undue delay. Where reasonably feasible and preliminary confirmed information is available, GloryScience will ordinarily issue an initial notification within seventy-two (72) hours after confirming a material security incident.

If the incident is complex, remains under investigation, involves a third-party cloud service provider or network service provider, is subject to forensic limitations, disclosure may increase security risks, or Applicable Law requires otherwise, GloryScience may supplement the notification in stages as further information becomes available.

The notification will include, to the extent reasonably known to GloryScience:

1. the nature of the incident;
2. the affected data types, system scope, or remote-access environment;
3. known or potential effects;
4. controls, mitigation measures, and remediation measures already taken or planned;
5. risk-mitigation measures recommended for the Customer; and
6. the method for further communication.

GloryScience may continue to supplement relevant information as the incident investigation, forensic work, and response progress.

The Customer shall promptly cooperate with GloryScience's incident investigation, including by providing necessary logs, configuration information, network information, contact support, Customer-side device information, alerts from Customer-side security tools, access records, and other reasonably necessary information.

Where information is delayed or incomplete, or an investigation is limited, due to a third-party infrastructure provider, cloud service provider, network operator, equipment vendor, Customer-side environment, or Force Majeure event, GloryScience will use commercially reasonable efforts, within reasonable limits, to provide relevant notices and updates.

Unless expressly required by Applicable Law or otherwise agreed by the parties in writing, a security-incident notice from GloryScience to the Customer does not constitute notice by GloryScience on the Customer's behalf to a regulatory authority, end user, subscriber, Customer employee, or other third party. As the party responsible for its

Tenant Data, networks, end-user relationships, and local regulatory obligations, the Customer shall independently determine and fulfill any applicable regulatory notice, customer notice, subscriber notice, or other legal obligation.

12. Personnel Security

GloryScience will apply reasonable management measures to personnel who access Customer Data or production systems, including:

1. confidentiality obligations;
2. access approval;
3. revocation of access following termination of employment or a change in role;
4. security-awareness training;
5. restrictions and supervision for privileged access; and
6. stricter permission management or operational auditing for personnel with access to high-risk systems, according to role requirements and commercial reasonableness.

GloryScience may use employees, personnel of Affiliates, contractors, or service providers to support service delivery, but will ensure that they are subject to appropriate confidentiality and security obligations when accessing Customer Data. If employees, personnel of Affiliates, contractors, or service providers access Customer Data, Tenant Data, remote-access data, logs, or other protected data from outside Hong Kong, GloryScience will implement appropriate access controls, confidentiality obligations, cross-border transfer safeguards, logging, and minimum-necessary access controls in accordance with the applicable DPA, Privacy Policy, Master Agreement, and Applicable Law.

13. Subprocessors and Third-Party Providers

GloryScience may use third-party service providers to support service operations, including:

1. cloud infrastructure providers;
2. payment processors;
3. logging and monitoring providers;
4. ticketing and customer-support systems;
5. email and communications providers;
6. security-tool providers;
7. AI service providers, where applicable; and
8. domain-name, CDN, identity-authentication, alert-notification, analytics, or other ancillary service providers.

GloryScience will take commercially reasonable measures to ensure that relevant service providers undertake data-protection, confidentiality, and security obligations appropriate to the nature of their services.

The notice and objection mechanism for changes to material Subprocessors shall be governed by the DPA, Privacy Policy, or Master Agreement. With respect to security controls, GloryScience may replace, suspend, or substitute relevant third-party providers as necessary for service continuity, security-incident response, vendor service discontinuation, legal-compliance requirements, or infrastructure adjustments, and will notify affected Customers where reasonably feasible.

14. AI Security and Data Use

Certain Oneasy features may use AI, machine learning, large language models, RAG, automated analysis, RCA-assisted analysis, or other AI-assisted capabilities.

Unless expressly authorized by the Customer in writing, GloryScience will not use identifiable Customer Data to train general-purpose artificial-intelligence foundation models.

GloryScience will take reasonable measures to reduce AI-related security risks, including:

1. restricting access to AI features;
2. avoiding unnecessary transmission of identifiable Customer Data to third-party AI services;
3. positioning AI outputs as assistive, advisory, or informational;
4. requiring the Customer to conduct human review before executing AI recommendations, configuration recommendations, RCA recommendations, or automated tasks in a production network; and
5. recording, to the extent commercially reasonable, key AI-related inputs, outputs, calls, approvals, or execution records to support security audits, troubleshooting, and dispute handling.

If the Customer independently configures, connects, or authorizes the use of its own third-party LLM API Key, model service, cloud service, plugin, or external AI service, the Customer shall independently review the relevant third-party service's terms of use, data-processing terms, cross-border transfer mechanisms, confidentiality obligations, security capabilities, and fees. Except for matters within GloryScience's control in the Oneasy Services, GloryScience does not control third-party AI providers selected by the Customer and is not responsible for their model training, data retention, output quality, compliance, availability, or security incidents.

The Customer shall not directly apply AI-generated content, RCA conclusions, configuration recommendations, script recommendations, or automation recommendations to a production network environment without human review and confirmation. The Customer shall bear losses arising from direct execution of AI output, including configuration errors, network outages, service failures, end-user complaints, or other losses, unless the loss was directly caused by GloryScience's willful misconduct or gross negligence and Applicable Law does not permit the relevant liability to be excluded.

If a Oneasy feature needs to invoke a third-party AI, model, cloud-model API, RAG service, vector database, or similar service selected by GloryScience, and that service will process identifiable Customer Data, Tenant Data, network operations and maintenance data, remote-access data, or AI input and output data, GloryScience will handle the relevant data transfers and provider management in accordance with the applicable DPA, Privacy Policy, Subprocessor mechanism, and Applicable Law. Unless otherwise provided in the applicable service description, DPA, Order Form, or Customer configuration, GloryScience will take commercially reasonable measures to require such third-party providers not to use identifiable Customer Data to train their general-purpose foundation models.

15. Customer Security Responsibilities

The Customer is responsible for the security of its own environment, accounts, networks, equipment, and use of the Services, including:

1. managing Authorized Users;
2. assigning appropriate permissions;
3. enabling MFA or other strong authentication measures where Oneasy supports the relevant functionality;
4. safeguarding passwords, API Keys, Tokens, VPN credentials, SNMP communities, device accounts, private keys, certificates, and other sensitive credentials;
5. configuring internal network segregation, firewalls, ACLs, allowlists, routing policies, and access controls;
6. maintaining the security of OLTs, ONUs, servers, firewalls, switches, routers, ACSs/NMSs, management network segments, and other Customer-side equipment;
7. regularly backing up critical business data and critical network configurations;
8. reviewing configuration changes, AI recommendations, automated tasks, batch tasks, script execution, and remote operations and maintenance activities;
9. ensuring that it has lawful authorization to access, manage, and operate relevant network equipment;
10. ensuring that MIBs, OIDs, SNMP walk results, CLI/API materials, OMCI materials, firmware materials, equipment-vendor internal documents, private-interface descriptions, scripts, packet captures, log samples, configuration templates, or other Third-Party Technical Materials uploaded, submitted, configured, referenced, or authorized for use through Oneasy have a lawful source, sufficient authorization, and necessary confidentiality permissions;
11. avoiding the uploading, Processing, or storage through Oneasy of unlawful surveillance data, unauthorized intercepted communications data, data that violates communications-secrecy laws, or highly sensitive data that should not be submitted to Oneasy;
12. promptly revoking or replacing credentials after service termination, personnel changes, credential leakage, permission changes, or a security incident; and
13. designating a security contact and providing timely cooperation in the event of a material security incident, remote-access anomaly, or high-risk operation.

The Customer shall independently assess the effects of configuration changes, automated operations, batch tasks, and remote operations and maintenance activities on its network environment and shall be responsible for the consequences of such operations. As the party responsible for its networks, equipment, end-user relationships, and local regulatory obligations, the Customer shall independently comply with applicable telecommunications regulation, cybersecurity, data protection, communications secrecy, critical-infrastructure, or similar legal requirements.

16. Security Documentation and Audit Support

Upon the Customer's reasonable request, GloryScience may provide security materials relating to the Oneasy Services that it may disclose publicly or under confidentiality obligations, including:

1. a security-controls overview or security white paper;
2. a summary of technical and organizational measures (TOMs);
3. a Subprocessor summary;
4. a description of data Processing and data flows;
5. a summary of the security-incident handling process;
6. a summary of the vulnerability-management process;
7. a penetration-test summary or third-party security-assessment summary, if available and disclosable;
8. available security certifications, reports, or third-party assessment summaries, if any;
9. reasonable responses to enterprise-customer security questionnaires; and
10. other enterprise audit-support materials agreed by the parties in writing.

Unless otherwise agreed by the parties in writing, GloryScience is not obligated to accept:

1. unrestricted on-site audits;
2. penetration testing of production environments;
3. unauthorized scanning, stress testing, red-team testing, or vulnerability verification;
4. access to internal systems related to GloryScience or the Oneasy Services, source code, models, prompts, infrastructure consoles, other Customers' data, or trade secrets;
5. audit requirements that affect platform security, stability, service continuity, or the rights and interests of other Customers; or
6. excessively frequent, unreasonable, repetitive audit requests or requests unrelated to the Customer's actual compliance needs.

Any additional audit, specific security assessment, customized Customer compliance support, regulatory-cooperation support, on-site audit, in-depth questionnaire, preparation of evidentiary materials, or report in a Customer-specified format shall be separately agreed by the parties in writing and may be subject to additional fees.

17. Data Deletion and Secure Disposal

Following closure of the Customer account, termination of the Services, expiration of the applicable data-export period, or a valid deletion request made by the Customer under the Master Agreement, DPA, or Applicable Law, GloryScience will handle Customer Data in accordance with the Master Agreement, Privacy Policy, DPA, and Applicable Law.

The general position is as follows:

1. the Customer may ordinarily export Tenant Data within thirty (30) days after service termination or account closure, unless otherwise provided by the Master Agreement, an Order Form, the DPA, or Applicable Law;
2. after service termination, GloryScience will initiate and complete a commercially reasonable process to delete or anonymize production-environment Tenant Data within ninety (90) days;
3. backup data, security logs, audit logs, material security-incident logs, financial records, data subject to statutory retention, data required for dispute resolution, and data that Applicable Law permits or requires to be retained are excluded;
4. with respect to Tenant Data in backup systems, GloryScience will not ordinarily delete data for a single Customer separately from historical backup media, but the relevant data will be progressively deleted or rendered irrecoverable according to established backup rotation, overwrite, or expiration cycles;
5. retained data will be processed only to the extent necessary for compliance, security, dispute resolution, backup recovery, audit, financial records, or performance of legal obligations; and
6. GloryScience may use deletion, anonymization, overwriting, isolation, access restriction, or other commercially reasonable methods for secure disposal.

18. Business Continuity

GloryScience will establish and maintain commercially reasonable business-continuity and disaster-recovery plans to reduce the risk of material service interruption.

Unless the parties separately sign an SLA, Order Form, or specific agreement, any business-continuity plan, RTO, RPO, recovery objective, description of recovery procedures, backup-and-recovery arrangement, or disaster-recovery plan does not constitute a legally binding service-level commitment.

For medium-sized and large enterprise Customers, regulated Customers, or critical business scenarios, the parties may separately agree through an Enterprise SLA, specific security addendum, or Order Form on specific availability, support-response, RTO, RPO, service-credit, testing, or reporting obligations. Any such additional commitment must be agreed in writing.

19. Limitations

This Security Addendum does not constitute a commitment that:

1. the Oneasy Services are absolutely secure;
2. the Oneasy Services will never be interrupted;
3. data will never be lost;
4. a security incident will never occur;
5. GloryScience or the Oneasy Services assumes security responsibility for Customer-side networks, equipment, configurations, credentials, permissions, third-party systems, or end-user services;
6. GloryScience or the Oneasy Services has obtained any security certification not expressly stated;
7. GloryScience guarantees that the Customer's production network, OLTs/ONUs, end-user services, equipment compatibility, AI/RCA results, or automated-task results will not experience failures, errors, interruptions, or losses; or

8. GloryScience assumes the Customer's non-transferable statutory obligations as an ISP, telecommunications carrier, network operator, critical-infrastructure operator, or party subject to local regulatory obligations.

The limitations of GloryScience's liability under this Security Addendum are governed by Section 9 of the Oneasy SaaS Service Agreement, except for liability that Applicable Law expressly prohibits from being limited.

20. Governing Law and Dispute Resolution

The governing law and dispute-resolution mechanism for this Security Addendum are governed by Section 12 of the Oneasy SaaS Service Agreement.

21. Order of Precedence

If this Security Addendum conflicts with another document, this Security Addendum shall prevail with respect to security controls, security-incident response, technical and organizational security measures, remote-access security, Agent/VPN security, vulnerability management, log retention, AI security, and Customer security responsibilities. If any such matter also involves Personal Data Processing, cross-border transfers, Subprocessors, Data Subject Requests, Personal Data Breach notification, or obligations under Data Protection Laws, the specific provisions of the DPA shall prevail.

If different documents conflict, unless the parties expressly agree otherwise through an Order Form, SOW, Enterprise SLA, or other authorized written document, the following order of precedence applies:

1. Order Form / Subscription Order / SOW / Enterprise SLA;
2. Data Processing Agreement / DPA;
3. Security Addendum;
4. Oneasy SaaS Service Agreement;
5. Oneasy Payment and Refund Terms;
6. Oneasy Privacy Policy;
7. Oneasy Cookie Policy; and
8. Oneasy Website Terms of Use.

However, the Payment and Refund Terms shall govern matters solely concerning payments, refunds, billing, automatic renewal, chargebacks, and overdue payments; the Website Terms of Use shall govern access to the public website; the Cookie Policy shall govern Cookies and tracking technologies; the DPA shall govern Personal Data Processing matters; and the Security Addendum shall govern security-control matters, except that where a security matter also involves Personal Data Processing, cross-border transfers, Personal Data Breach notification, or obligations under Data Protection Laws, the DPA shall prevail.

Annex A - Security Control Matrix

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
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

This checklist sets out Customer-side security responsibilities and recommended measures. Unless otherwise agreed by the parties in writing, it does not create any obligation for GloryScience to audit, supervise, verify, or continuously monitor the Customer-side environment.

The Customer shall take at least the following measures:

1. enable MFA for administrator accounts and privileged users where Oneasy supports the relevant functionality;
2. use strong passwords and change them periodically;
3. control API Keys, Tokens, SNMP communities, device accounts, private keys, certificates, and VPN/Agent credentials;
4. promptly remove users who no longer require access;
5. restrict the network scope accessible by the VPN/Agent;
6. segregate OLT/ONU management network segments;
7. use firewalls, ACLs, allowlists, dedicated accounts, or bastion hosts to restrict access;
8. review AI recommendations, automated tasks, batch configuration operations, and high-risk changes;
9. back up critical configurations and prepare a rollback plan before material configuration changes;
10. periodically review operational logs and remote-access logs;
11. promptly install Agent/VPN security updates or implement recommended mitigation measures;
12. promptly revoke or rotate credentials after personnel changes, service termination, or suspected leakage;
13. designate a security contact and cooperate with security-incident investigations;
14. ensure that devices, networks, and data connected to Oneasy are lawfully authorized;
15. not submit MIBs, OIDs, SNMP walk results, CLI/API materials, OMCI materials, firmware materials, equipment-vendor internal documents, private-interface descriptions, scripts, packet captures, log samples, configuration templates, or other Third-Party Technical Materials that are of unknown origin, that the Customer has no right to disclose, copy, or sublicense, or that are subject to third-party confidentiality restrictions; and
16. not upload unlawful surveillance data, unauthorized intercepted communications data, data that violates communications-secrecy laws, or highly sensitive data that should not be submitted to Oneasy.

Annex C - Remote Access Control Schedule

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
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