Oneasy SaaS Service Privacy Policy

Last Updated: June 25, 2026

Effective Date: June 25, 2026

GloryScience International Limited, a company incorporated under the laws of the Hong Kong Special Administrative Region (hereinafter referred to as "**GloryScience**," "**we**," "**us**," or the "**Company**"), is the operating entity of the Oneasy SaaS Platform (hereinafter referred to as "**Oneasy**" or the "**Service**"). We recognize the importance of personal information to you and are committed to providing reasonable and appropriate protection commensurate with the nature of the Service. This SaaS Service Privacy Policy (the "**Policy**") is intended to explain clearly and transparently how GloryScience processes your personal information when you use the Oneasy website, the Oneasy SaaS service platform, or otherwise interact with us.

This Policy forms part of the Oneasy SaaS Service Agreement (the "**Master Agreement**"). With respect to personal data processing matters, if this Policy conflicts with the Master Agreement, the applicable data processing agreement executed by the parties or incorporated by reference (if applicable), or the mandatory requirements of Applicable Law shall prevail. With respect to specific security controls, remote access security, incident response, log retention, and technical and organizational measures, the applicable Security Addendum, DPA, or other security document separately agreed by the parties shall prevail. Your specific rights and obligations are ultimately determined by Applicable Data Protection Law having jurisdiction over you or the relevant processing activities, as well as by any regional supplemental terms that we may issue. Please read this Policy carefully before using our Service. If you do not agree with any part of this Policy, do not use our Service.

Article 1 Scope and Role Definitions

1.1 Scope of This Policy

This Policy applies when you use or access the following services provided by us: the Oneasy website, including www.oneasy.cc and its subdomains; the Oneasy SaaS service platform; and related APIs, support channels, and sales communications.

This Policy does not apply to any website, application, or service operated by a third party, even if you access it through our Service.

1.2 Definitions of Key Roles

Under major data protection laws worldwide, we may perform the following legal roles in different data processing scenarios:

(A) GloryScience as a "Data Controller" (Controller)

For personal information that must be processed in order to provide, operate, protect, and improve our Service, we may act as a Data Controller. This generally includes: your account information; billing and transaction information; service usage logs and diagnostic data; security and compliance logs; and information collected through Cookies and similar technologies for website operation, analytics, security protection, and service optimization.

(B) GloryScience as a "Data Processor" (Processor)

For any data that you, as our "Tenant," upload, generate, or manage while using the Oneasy Service ("**Tenant Data**"), GloryScience generally acts as a Data Processor. Tenant Data may include information about devices you manage, network configurations, performance metrics, and operations and maintenance logs. In this role, GloryScience processes Tenant Data only in accordance with the Master Agreement, the DPA, and your configuration instructions within the Service. With respect to Personal Data contained in Tenant Data, GloryScience's specific obligations as a Data Processor shall be governed by the applicable DPA.

(C) The Tenant as a "Data Controller"

As a Tenant, you are the Controller or equivalent responsible party for your Tenant Data and are independently responsible for complying with all privacy, data protection, confidentiality of communications, telecommunications regulation, cybersecurity, and other related laws applicable to your data processing activities, including ensuring that you have a lawful basis for processing such data.

1.3 Interpretation of Roles in Non-GDPR Jurisdictions

Where Applicable Law does not use the terms “Controller / Processor,” or where the relevant terms have different meanings, references in this Policy to Controller, Processor, Tenant, and Service Provider shall be interpreted according to the functionally closest roles and obligations under that law; however, such interpretation shall not expand GloryScience’s statutory obligations beyond the scope expressly prescribed by Applicable Law.

Article 2 Information We Collect

We follow the principle of data minimization and collect only information necessary for specific, explicit, and lawful purposes.

2.1 Account and Configuration Information

To create and manage your account, we collect your name, email address, password, and any information that you choose to provide, such as your job title, department, company information, account role, and permission settings.

2.2 Subscription and Payment Information

To process subscriptions and payments, we collect your company name, billing address, taxpayer identification number, order records, subscription plan, payment status, and invoice-related information. Payment details, such as complete credit card information, are processed directly by industry-standard third-party payment service providers designated by us, and we do not store complete payment card information.

2.3 Service Usage and O&M Data

To ensure proper operation of the Service, troubleshoot faults, and improve performance, we automatically collect IP addresses, device identifiers, browser types, access timestamps, feature usage logs, performance metrics, error reports, login records, API call records, security incident records, and other necessary Platform Operational Data.

2.4 Tenant Data

All business data that you enter, upload, configure, authorize the Service to read, permit the Service to generate, or that the Service generates based on your devices, network, or configurations while you use the Service constitutes Tenant Data. You control the specific content of Tenant Data, and we, as Processor, are not responsible for its content. The Tenant shall independently determine whether the data that it uploads, connects, transmits, processes, or authorizes GloryScience to process through the Oneasy Service is restricted by applicable telecommunications regulatory laws, confidentiality of communications laws, cybersecurity laws, or data protection laws.

Tenant Data may include configuration information for ISP network devices, IP addresses, MAC addresses, device identifiers, OLT / ONU information, network topology, operations and maintenance logs, fault and alarm records, performance metrics, telemetry data, remote access logs, SNMP walk results, CLI / API output, configuration backups, packet-capture files, diagnostic results, or parsing results. In certain jurisdictions, such data may be regarded as Personal Data, regulated telecommunications data, communications metadata, cybersecurity data, commercially sensitive information, or data relating to critical infrastructure. The Tenant shall make its own determination and bear the corresponding compliance responsibilities.

A Customer’s acceptance of the Master Agreement, creation of a Tenant, addition of devices, configuration of credentials, enablement of Agent / VPN / Connector / API / SNMP / TR-069 / TR-369 / CLI / Syslog / ACS / NMS interfaces, uploading or submission of MIBs, OIDs, SNMP walk results, CLI / API output, configuration backups, logs, packet-capture files, scripts, templates, device materials, vendor materials, or other Third-Party Technical Materials, or authorization for Oneasy to read, generate, or process such materials, constitutes, for purposes of personal data protection, the Customer’s instruction and authorization to GloryScience to process the relevant Tenant Data.

For the avoidance of doubt, this Policy primarily describes the processing of personal information and the portions of Tenant Data that constitute Personal Data. Except for portions containing Personal Data, the provenance of rights, authorization for use, confidentiality obligations, intellectual property rights, trade secret restrictions, and allocation of responsibility for MIBs, OIDs, SNMP walk results, CLI / API materials, OMCI materials, firmware materials, device vendor materials, vendor internal documents, configuration templates, scripts, packet-capture files, log samples, or other Third-Party Technical Materials that a Customer provides, uploads, submits, configures, references, authorizes GloryScience to read, or permits the Service to generate through the Oneasy Service shall be

governed by the Master Agreement, Security Addendum, Order Form, SOW, or specific terms applicable to technical materials.

2.5 Communication Records

When you contact our support team, participate in a sales consultation, submit a support ticket, attend training, or provide feedback, we retain the relevant communications, attachments, and diagnostic information that you voluntarily provide.

2.6 Sensitive Personal Information

If you believe that a use case unavoidably involves sensitive personal information, special categories of Personal Data, communications content, or other highly sensitive data, you must obtain GloryScience's express written consent before submitting such data and confirm that you have all necessary lawful bases, notices, consents, authorizations, filings, or approvals. GloryScience may refuse to process such data for reasons relating to security, compliance, technical feasibility, or commercial risk.

2.7 Cookies and Similar Technologies

We may use Cookies, log identifiers, and similar technologies to enable website operation, maintain login status, provide security protection, retain necessary preferences, facilitate payment processes, prevent fraud, or comply with legal requirements. According to the current Cookie Policy, as of the date on which that policy was last updated, Oneasy does not currently enable non-essential analytics Cookies, advertising Cookies, marketing Cookies, remarketing Cookies, cross-site tracking Cookies, conversion tracking Cookies, or non-essential online chat / customer interaction Cookies. For information about Cookie types, purposes, retention periods, and management methods, please refer to our Cookie Policy.

Article 3 How We Use Your Information and the Legal Bases

We process your personal information only where we have a valid legal basis.

3.1 Performance of a Contract

Processing your account and payment information and providing the core SaaS functionality are necessary for the performance of the Master Agreement entered into with you.

3.2 Legitimate Interests

We process certain information on the basis of our legitimate interests, including monitoring the security of the Service, preventing fraud and abuse, improving the Service and conducting product research and development, maintaining platform stability, handling customer support requests, and carrying out necessary internal administration. To the extent required by Applicable Law, we will assess the impact of such processing activities on your privacy and take reasonable measures to reduce unnecessary privacy risks.

To the extent required by Applicable Law and reasonably practicable, we may provide descriptions of the relevant processing activities.

3.3 Compliance with Legal Obligations

We may process and retain your information where necessary to comply with tax, accounting, law enforcement, regulatory, security, dispute resolution, or other legal and regulatory requirements.

3.4 Consent

For processing activities that are not necessary for operation of the Service, such as certain marketing communications, we will obtain your consent where required by Applicable Law. You have the right to withdraw your consent at any time in accordance with Applicable Law.

Article 4 Processing of Tenant Data

4.1 Processing Principles

We process Tenant Data only in accordance with the Master Agreement, the applicable DPA, Security Addendum, Order Form, SOW, product functionality, and your configurations, uploads, authorizations to read, permissions to generate, or other recorded instructions within the Service. Your actions in adding devices, configuring credentials, enabling Agent / VPN / Connector / API / SNMP / TR-069 / TR-369 / CLI / Syslog / ACS / NMS interfaces, uploading or submitting files, authorizing the reading of device output, or permitting the generation of SNMP walk results, CLI / API output, configuration backups, packet captures, logs, or diagnostic results may each constitute your in-Service instruction to process the relevant Tenant Data.

If we receive an instruction that manifestly violates applicable data protection law, we reserve the right to refuse to carry out that instruction. If we believe that an instruction may violate Applicable Law, we will, to the extent reasonably practicable, notify you and explain the reasons, and give you a reasonable opportunity to provide a legal basis or an alternative solution. The parties shall consult in good faith to seek an alternative solution that complies with legal, contractual, and service security requirements. If no resolution is reached and we reasonably believe that carrying out the instruction would expose us to legal liability or security risk, or cause us to violate third-party obligations, we may suspend performance of the relevant instruction, and such suspension shall not constitute a breach of contract.

4.2 Tenant Responsibilities

You represent and warrant that you have the lawful rights and bases necessary to process all Tenant Data; that you have provided all privacy notices required by law to Data Subjects, subscribers, End Users, employees, or other relevant persons; that you have obtained all necessary consents, authorizations, permits, filings, internal approvals, or other lawful bases; and that you have implemented appropriate internal permission management, network segregation, and security controls.

With respect to devices, networks, interfaces, accounts, credentials, MIBs, OIDs, SNMP walk results, CLI / API output, OMCI materials, firmware materials, configurations, logs, packet captures, scripts, templates, or other Third-Party Technical Materials accessed, configured, authorized to be read, permitted to be generated, or processed through the Oneasy Service, you shall independently confirm and obtain all necessary ownership rights, rights of operation, management rights, authorized operations and maintenance rights, rights of disclosure, rights of reproduction, rights of use, rights of sublicensing, confidentiality waivers, device vendor licenses, contractual authorizations, regulatory permits, and End User notices or consents. We may reasonably rely on your in-Service configurations, uploads, submissions, authorizations to read, permissions to generate, and operation records without separately verifying your chain of authorization before each processing activity.

4.3 Assistance Obligations

If a Data Subject seeks to exercise rights directly against us in relation to Tenant Data, such as a request for access, correction, deletion, or restriction of processing, we will generally direct that person to contact you as the Controller or responsible party for the relevant data. Within reasonable limits, we will assist you in fulfilling your applicable statutory obligations to Data Subjects through product functionality, APIs, export functionality, or technical support.

Article 5 International Data Transfers

Our Service is global in nature, which means that your personal information may be accessed, processed, or transferred outside the country or region in which you are located.

5.1 Our Safeguards

When personal information is transferred from your jurisdiction to another region and applicable data protection law requires safeguards for cross-border transfers, we will use legally recognized data transfer mechanisms, such as the European Union Standard Contractual Clauses (SCCs), an international data transfer mechanism applicable in the United Kingdom, or another applicable mechanism, together with reasonable technical and organizational measures, such as access controls, encryption, logging, and security monitoring, to provide protection.

5.2 Cross-Border Transfers of Tenant Data

By default, the primary storage region for Tenant Data is the Alibaba Cloud International Singapore Region. In order to provide the Service, improve access performance, support disaster recovery, provide security protection and technical support, enable Subprocessor services and AI-assisted functionality, provide access through regional secondary nodes, or comply with legal obligations, the relevant data may be accessed, processed, cached, backed up, or transferred in other jurisdictions.

We may use Alibaba Cloud International and other assessed providers of cloud infrastructure, network, CDN, security, logging, monitoring, payment, customer support, and AI services as Service Providers or Subprocessors. A list of material Subprocessors, together with their service categories, processing purposes, and primary processing locations, will be published or made available through the official Oneasy website, administrative console, documentation pages, or other reasonable means.

The specific data regions, secondary nodes, disaster recovery nodes, edge nodes, log nodes, cache nodes, backup nodes, support access locations, Subprocessor processing locations, and AI service invocation locations shall be governed by the applicable Master Agreement, DPA, Security Addendum, Order Form, service configuration, Subprocessor list, or written agreement between the parties. Unless the parties expressly agree otherwise in writing, the description of a primary storage region in this Policy does not constitute a data localization commitment and does not guarantee that all access, processing, caching, backups, logging, technical support, or Subprocessor services will occur only in a single jurisdiction.

The Customer is solely responsible for completing any transfer impact assessment, adequacy assessment, notification, consent, filing, or other compliance procedure required of it as Controller or equivalent responsible party. This Section does not affect the necessary cross-border processing by us, as Data Controller, of account, log, payment, support, compliance, and Platform Operational Data for the purposes described in Article 3.

Article 6 Information Sharing and Disclosure

We do not sell your personal information. We share information only in the following circumstances:

- **Service Providers / Subprocessors:** We may share necessary information with partners that provide us with cloud hosting, network, CDN, payment, analytics, communications, security, logging, monitoring, customer support, AI services, or other necessary services (“**Subprocessors**” or “**Service Providers**”). Such partners may include Alibaba Cloud International and other assessed providers of cloud infrastructure, network, security, logging, monitoring, payment, customer support, and AI services. We will take commercially reasonable measures to require the relevant Service Providers to assume confidentiality, data protection, and security obligations commensurate with the nature of their services. For material Subprocessors involved in the processing of Tenant Data, the notification, objection, and change mechanisms shall be governed by the applicable DPA, Master Agreement, or other applicable document.

  GloryScience’s current list of material Subprocessors, together with their service categories, processing purposes, and primary processing locations, will be published or made available through the official Oneasy website, administrative console, documentation pages, or other reasonable means. When GloryScience adds or replaces a material Subprocessor that may have a material effect on the processing of Tenant Data, GloryScience will notify the Customer and provide a reasonable objection mechanism in accordance with the applicable DPA, Master Agreement, or other applicable document.
- **Legal Requirements:** We may share information in response to valid legal process, regulatory requirements, law enforcement requests, or court orders; to protect personal safety; to defend the lawful rights or property of us, our Customers, or third parties; or where otherwise required by law.
- **Business Reorganization:** In connection with a corporate merger, acquisition, financing, sale of assets, transfer of business, restructuring, or similar transaction, we may disclose relevant information to the extent necessary, but will take reasonable measures to ensure that your information remains subject to appropriate confidentiality and data protection obligations.

Article 7 Data Security

7.1 Security Standards

We will implement and maintain commercially reasonable technical and organizational security measures to protect personal information and Tenant Data against unauthorized access, disclosure, alteration, loss, or destruction. Such measures may include access controls, authentication, encryption in transit, protection of data at rest where appropriate, logging and monitoring, vulnerability management, personnel confidentiality obligations, and incident response processes.

Specific security controls, remote access security, Agent / VPN security, log retention, vulnerability management, security audit support, and technical and organizational measures shall be governed by the Oneasy Security Addendum, the DPA, the Master Agreement, or a security document separately agreed by the parties.

7.2 Security Incident Notification

If we confirm a security incident that may have a material impact on your personal information, Tenant Data, or the security of the Service, we will notify you to the extent required by law and without undue delay. Where reasonably practicable and preliminary confirmed information is available, we will generally issue an initial notice to the Customer within seventy-two (72) hours after confirming a material security incident.

To the extent reasonably known to us, the notice will include the nature of the incident; the categories of affected data or the scope of affected systems; known or potential effects; the containment, mitigation, and remediation measures that we have taken or are taking; risk mitigation measures recommended for the Customer; and channels for further communication. We may continue to supplement the relevant information as the investigation, forensic analysis, and response progress.

7.3 Backup and Recovery

We will implement reasonable data backup strategies based on business needs and generally accepted industry practices. If specific backup frequencies, retention periods, recovery procedures, recovery time objectives (RTOs), or recovery point objectives (RPOs) are to constitute legally binding commitments, they must be set forth in an applicable SLA, Order Form, Security Addendum, or specific agreement separately executed or incorporated by reference by the parties. Unless expressly agreed otherwise, RTOs and RPOs do not constitute legally binding service-level commitments.

7.4 User Security Responsibilities

You understand and agree that the Internet, cloud services, and remote access environments are not absolutely secure. You must properly manage accounts, permissions, administrator identities, API Keys, access tokens, VPN / Agent credentials, device credentials, network segregation policies, and internal approval processes.

Except where Applicable Law mandatorily requires otherwise or the parties expressly agree otherwise, we are not responsible for any data breach, network interruption, or loss resulting from your failure to safeguard account credentials, improper actions by Authorized Users, improper permission configuration, insufficient network segregation on the Customer side, vulnerabilities in Customer-side devices or systems, failure to update Agent / VPN components promptly, or your choice to access the Service through a network environment that does not meet security requirements. We strongly recommend that you enable multi-factor authentication (MFA) for administrator accounts, periodically review Authorized Users and permissions, and regularly rotate API Keys, access tokens, and privileged credentials.

7.5 Data Retention

We retain personal information and Tenant Data only for the period necessary to achieve the purposes described in this Policy, the Master Agreement, the applicable DPA, the Security Addendum, or Applicable Law. Specific retention periods, deletion, anonymization, export, and exceptional retention rules for account information, Tenant Data, operations logs, security logs, backup data, financial records, and dispute resolution materials shall be governed by the Master Agreement, the applicable DPA, the Security Addendum, system configuration, or the requirements of Applicable Law.

Article 8 Your Data Subject Rights

Depending on the data protection laws applicable to you, you may have the rights to access, correct, or delete Personal Data; restrict processing; exercise data portability; withdraw consent; and object to certain processing activities.

How to Exercise Your Rights: If you are an Authorized User of a Tenant, please first contact the account administrator of your organization. If you are the direct Controller of the account, or the administrator is unable to handle your request, please email **support@oneasy.cc**. For security purposes, we may verify your identity before processing the request.

For requests made by Tenant Authorized Users or Data Subjects in relation to Tenant Data, the Tenant, as the Controller or responsible party for the relevant data, shall handle and respond to such requests in a timely manner in accordance with Applicable Law. GloryScience will, within reasonable limits, assist the Tenant in fulfilling its applicable obligations through the product functionality of the Oneasy Service, APIs, export functionality, or technical support.

For personal information that GloryScience processes as Controller, we will respond to a verifiable request within the time period prescribed by Applicable Law. To the extent permitted by Applicable Law, we may refuse or limit requests for information that are manifestly unfounded, excessively repetitive, adversely affect the rights of others, involve trade secrets or security risks, or concern information whose disclosure is prohibited by law.

Article 9 Disclaimers and Limitation of Liability

9.1 Service Provided "As Is"

To the maximum extent permitted by Applicable Law, our Service and all related content are provided on an "**AS IS**" and "**AS AVAILABLE**" basis. Except for matters expressly committed to in the Master Agreement, DPA, Security Addendum, or another written agreement between the parties, we make no express or implied warranties, including, without limitation, warranties of merchantability, fitness for a particular purpose, non-infringement, uninterrupted operation, or error-free operation. However, this Section does not limit liability arising from GloryScience's willful misconduct or gross negligence, or any liability that Applicable Law prohibits from being limited.

9.2 Disclaimer for Specific Circumstances

Except where Applicable Law mandatorily requires otherwise or the parties expressly agree otherwise, we are not responsible for any interruption, delay, loss of data, damage, or inability to access the Service directly or indirectly resulting from:

1. Force majeure events beyond our control, such as natural disasters, war, civil unrest, large-scale cyberattacks, telecommunications backbone outages, major public cloud failures, or regulatory restrictions;
2. Actions by you or your Authorized Users, device failures, network connectivity issues, improper permission configuration, credential compromise, insufficient internal approvals, or failure to follow security recommendations;
3. Your failure to follow our service configuration guides, technical documentation, security recommendations, or reasonable operating procedures;
4. Scheduled or emergency maintenance conducted for reasonable system maintenance, upgrades, security remediation, or emergency risk response;
5. Failure of any third-party service, Customer-side network, Customer device, device vendor firmware, private interface, third-party cloud service, or telecommunications service provider.

9.3 Allocation of Responsibility

The allocation of responsibility in relation to data processing, security incidents, or limitations of liability concerning the Oneasy Service shall be governed by the applicable Master Agreement, DPA, Security Addendum, and Applicable Law between GloryScience and the Customer.

Article 10 Governing Law, Dispute Resolution, and Independent Compliance Commitments

10.1 Governing Law

The interpretation, validity, and enforcement of this Policy, and any dispute arising from this Policy, shall be governed by the **laws of the Hong Kong Special Administrative Region**, without regard to any conflict-of-laws rules.

10.2 Compliance with Data Protection Laws

To the extent that the relevant laws apply to and have jurisdiction over GloryScience, GloryScience will comply with the mandatory requirements imposed on it by applicable data protection laws, including, where applicable, the EU GDPR, UK GDPR, Hong Kong PDPO, Singapore PDPA, and other Applicable Laws. The foregoing statement shall not be interpreted as GloryScience unconditionally accepting the application of the laws of any jurisdiction that has no genuine connection with the relevant processing activities.

Any conflict concerning governing law or dispute resolution shall remain subject to Section 10.1 of this Policy and the Master Agreement; however, those provisions do not affect a Data Subject's ability to lodge a complaint with a competent supervisory authority or exercise any non-waivable rights under Applicable Law.

10.3 Dispute Resolution

Any dispute arising out of or relating to this Policy shall be handled in accordance with the dispute resolution mechanism set forth in the Oneasy SaaS Service Agreement, including submission to arbitration administered by the Hong Kong International Arbitration Centre (HKIAC), if the Master Agreement adopts that mechanism. This arbitration provision does not affect a Data Subject's right to lodge a complaint with the relevant supervisory authority in accordance with law.

10.4 Policy Updates

We may revise this Policy from time to time. For materially adverse changes, including a material expansion of the scope of personal information collected, a new material sharing arrangement with a third party, a significant reduction in personal information protection standards, or a change that has a material adverse effect on Data Subject rights, we will notify the Tenant administrator thirty (30) days in advance by email, through the administrative console, by website notice, or by other reasonable means.

If Applicable Law requires a shorter or longer notice period, or if a change must take effect more quickly for security, legal, regulatory, service continuity, or emergency risk response reasons, we may proceed in accordance with Applicable Law and reasonable commercial practices. Continued use of the Service after the new Policy takes effect constitutes acceptance of the updated Policy. If a User does not agree, the User must stop using the Service and may handle termination or data export matters in accordance with the Master Agreement.

Article 11 Contact Us

If you have any questions about this Policy or our privacy practices, please contact our data protection team using the following details:

Legal and Data Protection Matters: legal@oneasy.cc

General Technical Support Matters: support@oneasy.cc

Mailing Address: NEW TREND CTR, NO. 704 PRINCE EDWARD RD EAST, SAN PO KONG, HONG KONG
