

Oneasy AI Agent Services Governance and Use Rules

Special Addendum to the Oneasy SaaS Service Agreement

Important Notice

1. Oneasy AI Agent Capabilities are intended to assist with knowledge retrieval, information understanding, analysis, diagnostics, drafting and workflow collaboration. They do not replace the final judgment of appropriately authorized and qualified engineers, security personnel, managers or the Customer.
2. AI Agent Output may be incomplete, inaccurate, outdated, erroneous, misleading, omit material information, lack sufficient context or fail to account for device-specific compatibility. Appropriate human review and internal approval are required for matters involving production networks, high-risk network operations, regulatory or contractual matters, security incidents or external publication.
3. AI Agent conversations, natural-language instructions, parameter pre-filling, general confirmations or acceptance of recommendations do not, by themselves, constitute valid authorization for External Execution or changes to a production network.
4. The Customer retains ultimate control over its networks, devices, data, business processes, Authorized Users and production changes. This paragraph does not exclude or limit any obligation of GloryScience under the Master Agreement, an applicable Data Processing Agreement, Security Addendum, other written agreement or mandatory law.

1. Purpose, Scope and Relationship with Other Documents

1.1 Purpose and Legal Effect

These Oneasy AI Agent Services Governance and Use Rules (these “Rules”) govern data, permissions, human review, External Execution, production-network controls, prohibited uses and incident cooperation in connection with the Customer’s and its Authorized Users’ use of Oneasy AI Agent Capabilities.

These Rules are a special addendum to the Oneasy SaaS Service Agreement (the “Master Agreement”). Once these Rules are expressly incorporated by reference through an Order, subscription page, administrative console, in-product checkbox, feature-enablement process or another recordable method, and are validly accepted by the Customer or its authorized representative, these Rules form an integral part of the Master Agreement.

Capitalized terms not defined in these Rules have the meanings given to them in the Master Agreement.

1.2 Persons and Capabilities Covered

These Rules apply to:

- Customers that have subscribed to, enabled, accessed or actually used Oneasy AI Agent Capabilities;
- the Customer’s Tenant Administrators and Authorized Users; and

- systems integrators, managed operations teams, consultants, contractors or other third parties lawfully authorized by the Customer to use AI Agent Capabilities within the Customer's tenant.

These Rules apply only to AI Agent Capabilities that have been officially released, are included within the Customer's subscription or trial, and are actually enabled in the Customer's tenant. The applicable functions, models, knowledge bases, interfaces, data scope and service status are determined by the Order, official product documentation, release notes, service configuration and actual enablement status.

Names of AI agents, brand architecture, demonstrations, marketing materials, roadmaps or conceptual descriptions do not constitute a commitment to deliver any unreleased, unordered or disabled capability, or any commitment regarding its performance, compatibility, accuracy, service outcome or continued availability.

1.3 Relationship with Other Documents

These Rules supplement the Master Agreement with respect to Customer Input, human review, data and permission management, knowledge bases, third-party connections, External Execution, High-Risk Network Operations, prohibited uses and cooperation relating to AI Agent incidents.

Where more than one document applies:

1. An Order, Subscription Order, Statement of Work (SOW), Enterprise Service Level Agreement (Enterprise SLA), or other duly executed written agreement prevails only with respect to the subscription, pricing, term, deployment, implementation, support, service level or other specific matter that it expressly addresses;
2. matters involving personal data processing, cross-border transfers, subprocessors, data-subject requests or statutory data-protection obligations are governed by the applicable Data Processing Agreement (DPA) and mandatory law;
3. matters involving security controls, remote access, security incident response or other specific security requirements are governed by the applicable Security Addendum;
4. fees, payments, refunds, intellectual property, general limitations of liability, indemnification, termination, governing law and dispute resolution are governed by the Master Agreement and the corresponding applicable documents; and
5. these Rules shall not be construed to expand any service obligation, feature commitment, service level or liability that GloryScience has not expressly assumed under the Master Agreement, an Order, DPA, Security Addendum or SLA.

1.4 Management of Authorized Personnel and Third Parties

The Customer shall ensure that its Tenant Administrators, Authorized Users and authorized third parties are informed of and comply with these Rules before using AI Agent Capabilities. Through contracts, internal policies, permission settings or other reasonable measures, the Customer shall require third parties that it authorizes to use its tenant to assume confidentiality, security, permission, data-handling and High-Risk Network Operation obligations that are no less protective than those set out in these Rules.

A systems integrator, managed operations team or other entity that uses Oneasy on behalf of multiple end customers shall ensure that it has valid authorization from each relevant network owner, operator or data-responsible entity, and shall maintain reasonable segregation among the customers' tenants, accounts, data, credentials and operations.

2. Definitions

Term	Meaning
AI Agent Capabilities	Question answering, retrieval, analysis, visualization, recommendations, drafting, diagnostic assistance, task orchestration or other officially released and enabled AI-assisted functionality provided by Oneasy through artificial intelligence models, machine learning, retrieval-augmented generation (RAG), knowledge bases, tool calls, controlled interfaces, workflows or similar technologies.

Term	Meaning
AI Agent Output	Text, code, analysis, configuration recommendations, diagnostic approaches, root-cause inferences, task recommendations, charts, summaries, pre-filled parameters or other AI-generated content produced automatically or semi-automatically by AI Agent Capabilities.
Customer Input	Customer Content, customer network data, telecommunications operations data, third-party technical materials, prompts, files, logs, configurations, commands, screenshots, interface data or other information that the Customer or an Authorized User enters, uploads, connects, authorizes for access or instructs AI Agent Capabilities to process.
External Execution	An action that may alter a Customer or third-party system, data, device, permission, public content, business process or operational state, including an action initiated through an interface, tool, script, workflow, automation or remote access.
High-Risk Network Operations	Configurations, commands, scripts, automation, remote access or other operations that may affect a production network, end-user services, business continuity, cybersecurity, data integrity or regulatory compliance.
Operational Verification Sources	On-site data, approved change records, actual device-returned results, official device-manufacturer documentation, applicable law, contractual documents or other authorized records used to verify a particular device, network, task or incident.
Network Access Components	Connectors, VPNs, API tokens or other technical components expressly identified as network access components and used for device connectivity, cloud-to-edge access or remote operations. A component does not become an AI Agent Capability merely because its name includes the word "Agent."

3. Roles and Responsibilities

Party or Role	Principal Responsibilities
Customer	Is responsible, as applicable, for its business purposes, lawfulness of data, network and device authorizations, production changes, internal approvals, business continuity and management of authorized personnel; and shall ensure that it has all lawful authority required to use AI Agent Capabilities and connect relevant systems.
Tenant Administrator	Manages users, roles, AI Agent features, knowledge bases, data access, third-party connections and credentials; establishes human-review, change, External Execution and incident-response processes; and periodically removes permissions and connections that are no longer required.
Authorized User	Uses AI Agent Capabilities only within authorized permissions and legitimate work needs; verifies material output; and does not bypass approvals, access controls, data boundaries or production-network controls.
Authorized Third Party	Uses the relevant tenant and data only within the scope authorized by the Customer, and does not transfer one customer's credentials, data, knowledge bases, output or operations into another customer's environment.
GloryScience	Provides officially released and enabled capabilities within the agreed service scope, and applies the service, security, support and risk controls specified in the applicable documents. GloryScience may take reasonable measures, including restriction, suspension or degradation, in response to abnormal, high-risk or non-compliant use in accordance with the Master Agreement and applicable documents.

The Customer shall designate appropriately authorized, knowledgeable and internally approved persons to be responsible for production-network connections, External Execution, automation and other high-impact uses.

AI Agent Output, displays, alerts, inferences, recommendations or conversations do not, by themselves, constitute on-site facts, Customer approval, a device manufacturer's conclusion, a formal work order, an audit conclusion, a compliance conclusion or completed execution.

The Customer retains control over its final business decisions, internal approvals and production-network changes. This allocation of responsibility does not exclude or limit any obligation of GloryScience under the Master Agreement, an applicable DPA, Security Addendum, other written agreement or mandatory law, and does not relieve GloryScience of liability that it must bear under contract or law for its own breach, willful misconduct or gross negligence.

4. Capability Scope and General Limitations

4.1 Actual Availability

The actual availability of AI Agent Capabilities depends on the Customer's subscription or trial, service region, product feature status, role permissions, connected data, knowledge sources, feature settings, third-party dependencies and current service status.

The Oneasy website, brand materials, demonstrations, sales presentations, roadmaps, conceptual names or responses generated by an AI agent do not constitute a commitment regarding unordered functionality, a particular model, knowledge base or interface, compatibility with a particular device, any specified accuracy rate, a particular service outcome or continued availability.

4.2 Capability Categories and Boundaries

The following categories describe governance boundaries only and do not, by themselves, establish that a capability has been released or is included in the Customer's subscription:

Capability Category	Potential Uses	Specific Boundaries
Professional Knowledge Q&A	Knowledge queries concerning optical access networks, OLTs/ONUs, network operations, configuration methods, alarms and troubleshooting	An answer is not a formal conclusion of a device manufacturer, a compatibility commitment or a production-ready operating instruction. For a particular model, software version, command or parameter, the Customer shall verify official documentation and on-site conditions.
Platform Knowledge and Interface Guidance	Oneasy product explanations, operating guidance, page location and navigation assistance	Guidance may be based only on pages, permissions and features that are actually available. Page navigation, parameter pre-filling or a general confirmation shall not be treated as authorization for production execution.
Business Query and Analysis	Querying platform data through available interfaces and within the Customer's permissions, and summarizing, filtering, tabulating or visualizing actual returned results	Queries, analyses and charts shall be based only on actual returned data. Interfaces, parameters, device status, business data and execution results must not be fabricated. Where parameters are pre-filled, the Customer shall confirm or supplement them before they are processed through a controlled platform workflow.
Other AI-Assisted Capabilities	As specified in official product documentation, release notes, the Order, service configuration and actual enablement status	A capability that has not been officially released, ordered or enabled is not a delivery commitment.

4.3 Inherent Limitations

The Customer understands that AI Agent Output is generated automatically or semi-automatically from Customer Input, tenant data, knowledge sources, model capabilities and system configuration and may be affected by:

- information that is incomplete, inaccurate, outdated or inconsistent with the current state of a product, device or software;
- incorrect conclusions, omissions, hallucinations, reasoning errors or other uncertainty;
- differences among device models, software versions, MIBs, OIDs, CLIs, APIs, data models or on-site environments;

- insufficient context, missing data, abnormal interface responses or restrictions caused by permissions; and
- limitations arising from third-party models, knowledge bases, cloud services or external interfaces.

AI Agent Output is provided only to assist with information retrieval, understanding, analysis, diagnostics, visualization, operating guidance and solution drafting. It does not replace the final judgment of appropriately authorized and qualified engineers, security personnel, managers, legal counsel or compliance personnel.

5. Data, Accounts, Knowledge Bases and Third-Party Services

5.1 Lawful Authority and Data Minimization

1. The Customer may submit, authorize the processing of, or connect only data, networks, devices, systems and third-party technical materials for which it has lawful rights and for which it has completed all necessary notices, consents, authorizations, approvals or other lawful procedures.
2. The Customer shall follow the principles of purpose limitation, data minimization and least privilege. The Customer shall remove from logs, configurations, screenshots, work orders, packet captures and diagnostic materials any personal data, credentials and sensitive information that are not required for the relevant task.
3. The Customer shall not use AI Agent Capabilities to circumvent any notice, authorization, assessment, filing, confidentiality or security obligation that applies to it as a data controller, data user, network operator or other responsible party.
4. When processing relevant information for lawful network operations, support, security or compliance purposes, the Customer remains subject to the Master Agreement, the applicable DPA, purpose limitation, data minimization and access-control requirements.

5.2 Credentials and Sensitive Information

1. Complete passwords, private keys, access tokens, API keys, high-privilege VPN, SSH or SNMP credentials, payment credentials or other information that should not enter a model context must not be submitted through ordinary conversations, prompts, knowledge bases, ordinary attachments or uncontrolled files.
2. Where a product function requires access credentials, the Customer shall submit them through a controlled credential-management channel expressly designated by Oneasy and configure least privilege, validity periods, rotation, revocation and access controls in accordance with official product documentation.
3. Unless official product documentation, an applicable agreement and the service configuration expressly provide otherwise, the Customer shall not assume that credentials submitted through a controlled credential channel will be made available to an AI model or included in ordinary conversations, knowledge bases or uncontrolled logs.
4. The Customer shall apply account-security measures proportionate to the risk, including strong authentication where supported, role-based access control, credential rotation, removal of access following departure or role changes, and log review. Administrator accounts must not be shared or used by unauthorized persons.

5.3 Third-Party Models and Data Processing

1. Certain Oneasy AI Agent Capabilities may use third-party large language models, model APIs, embedding models, vector databases or other artificial intelligence services.
2. The relevant service providers, processing purposes, data categories, processing locations, retention arrangements, subprocessors and cross-border transfer mechanisms are specified in the applicable DPA, subprocessor list, Privacy Policy, AI data notice, Order, service configuration or other official document.
3. Unless the Customer expressly authorizes otherwise in writing, GloryScience will not use identifiable Customer Data to train general-purpose artificial intelligence foundation models made available to other customers or the public.
4. The commitment not to use Customer Data for training does not mean that Customer Input, attachments, query results or related context will not be processed by a third-party AI service for inference, embedding, retrieval, security monitoring or another purpose necessary to provide the relevant functionality. Such processing remains subject to the applicable documents and data-protection requirements.

5. The Customer shall not submit data, confidential information or regulated information that it is not entitled to provide to GloryScience or the relevant third-party AI service for processing.

5.4 Protected Data

Unless expressly permitted by an applicable agreement, product configuration and lawful basis, the Customer shall not submit:

- raw communications content or information subject to communications-secrecy obligations;
- state secrets or information that applicable law prohibits from being transferred across borders, outsourced or processed by a third party;
- restricted trade secrets that the Customer is not authorized to disclose;
- sensitive personal data or other strictly regulated data; or
- any information that the Customer is not entitled to disclose to GloryScience or a third-party model provider.

Where processing of protected data is necessary, the Customer shall first confirm that the lawful basis, applicable DPA or specific agreement, data region, permissions, retention arrangements and security controls satisfy its requirements.

5.5 Knowledge Bases, Prompts and Third-Party Technical Materials

1. The Customer's administrators shall manage the source, rights status, applicable scope, update responsibility, access roles and obsolete content of knowledge bases and prompts.
2. When uploading or requesting use of device-manufacturer materials, MIBs, OIDs, CLI/API documentation, firmware materials, configuration templates, packet captures, log samples or other third-party technical materials, the Customer shall ensure that it has the lawful right to obtain, disclose, reproduce, upload, process and authorize use of those materials.
3. The Customer shall not upload materials of unknown origin, materials subject to confidentiality obligations or device-manufacturer license restrictions, or materials that may infringe a third party's intellectual property, trade secrets, contractual rights, communications-secrecy obligations or other lawful rights.
4. Knowledge-base content, retrieved passages and model responses do not necessarily constitute the latest, complete or officially authoritative device-manufacturer documentation. For a specific model, software version, command, parameter or configuration, the Customer shall verify official documentation and on-site conditions.
5. Rights in the Customer's own prompts, knowledge-base materials and other Customer Content are governed by the Master Agreement provisions concerning intellectual property and Customer Content. These Rules do not alter the Master Agreement arrangements concerning GloryScience's proprietary system prompts, templates, workflows and platform capabilities.

5.6 Prompt Injection and Third-Party Connections

1. Instruction-like content contained in web pages, files, emails, search results, third-party tools, device-returned content or Customer Input may be untrusted.
2. The Customer shall not use such content to induce AI Agent Capabilities to disclose information, alter permissions, bypass rules, obtain cross-tenant access or perform an unauthorized operation.
3. Before adding or changing a third-party tool, system, device, data source, interface, plug-in or automation, the Customer shall define the business purpose, data scope, least-privilege permissions, users, responsible person, risks, stop mechanism and exit mechanism.
4. When a connection is no longer required, authorization is withdrawn, personnel depart, credentials become abnormal or a risk is identified, the Customer shall promptly restrict or revoke the connection and rotate affected credentials as appropriate.

5.7 Tenant Isolation and Records

1. The Customer shall not attempt to access another tenant, unauthorized content, platform-management capabilities, logs, interfaces, credentials or system resources.

2. If cross-tenant visibility, abnormal permissions or unintended data access is discovered, the Customer shall immediately stop the relevant activity and report it through the designated support or security channel. The Customer shall not increase the impact through continued queries, bulk downloads, distribution of screenshots, forwarding or broader testing.
3. The Customer's administrators shall retain Customer-side records proportionate to the risk for the creation, modification, suspension or revocation of accounts, roles, knowledge bases, connections, automation and high-impact configurations.
4. AI Agent conversation records do not replace internal approvals, work orders, change records, authorization records, on-site records or other controlled evidence required by the Customer.

6. Production Networks, External Execution and High-Risk Network Operations

6.1 General Principle

For matters involving OLTs, ONUs, CPEs, ports, VLANs, QoS, ACLs, authentication, routing, service templates, bulk provisioning or configuration, scripts, automated tasks, firmware, remote commands or any other matter that may affect a production network or end-user services, AI Agent Output may be used only as a candidate solution, analysis, recommendation or draft.

AI Agent Output shall not be treated as an approved, completed or production-ready operating instruction, or as a guarantee of an execution result.

6.2 Human Review Before Execution

Before carrying out a High-Risk Network Operation, the Customer shall ensure that appropriately authorized and qualified personnel verify at least:

- the target device, object, tenant, site and scope of impact;
- the device manufacturer, model and software or firmware version;
- the network topology, service dependencies and current operating state;
- the meaning of commands, scripts, parameters, templates and interfaces;
- the expected outcome, failure conditions, stop conditions and rollback method; and
- internal approvals, testing and validation, configuration backups, maintenance windows, on-site coverage, end-user notices and regulatory requirements.

The Customer shall apply more stringent review and approval under its internal policies to material, bulk, cross-region, deletion, shutdown, firmware, permission-related, irreversible or potentially service-disrupting operations.

6.3 Authorization for External Execution

1. Whether External Execution is available depends on the relevant function being officially released, included in the Customer's subscription, enabled in the Customer's tenant and expressly identified in official product documentation.
2. Unless expressly permitted by an Order, product configuration or written agreement between the parties, the Customer shall treat External Execution by AI Agent Capabilities as disabled and unauthorized.
3. An AI Agent conversation, a natural-language instruction, general expressions such as "execute" or "continue," parameter pre-filling, model recommendations or acceptance of a recommendation do not, by themselves, constitute valid authorization for production execution.
4. External Execution shall be completed only through a separate controlled mechanism provided by the product or through an external-system process approved by the Customer, and must satisfy applicable identity verification, role-permission, internal-approval, execution-confirmation and audit requirements.
5. To the extent supported by the product, the Customer shall apply secondary confirmation, step-up authentication, separation between requester and approver, or dual approval to material or high-risk operations.

6. The Customer shall not use AI Agent Capabilities to bypass network segregation, change approval, permission controls, maintenance windows or on-site safety controls.

6.4 Scope, Records and Stopping Execution

1. An automated or External Execution task shall have a defined objective, target, scope, least-privilege permissions, validity period, stop or revocation mechanism, execution record and result-verification process.
2. The Customer shall avoid directly translating open-ended, ambiguous or unbounded natural-language instructions into production execution.
3. Where the product provides relevant recording capabilities, the Customer shall use product logs together with its own controlled records to distinguish manually initiated actions, API-initiated actions, scheduled tasks, system-automated tasks, AI Agent recommendations and actual execution.
4. The Customer shall ensure that an available emergency path exists to terminate a task, revoke credentials, disconnect a connection, roll back a configuration or otherwise stop an operation. The specific capabilities available depend on actual product functionality, device compatibility and on-site conditions.
5. After execution, the Customer shall verify actual device-returned results, service status, scope of impact, failed objects and rollback results. AI Agent text or a conversation conclusion alone shall not be used as proof of completion.

6.5 Handling Abnormal Events

If an abnormal event occurs, results differ from expectations, the scope of impact is unclear, permissions are abnormal, cross-tenant visibility occurs, data is improperly disclosed, or dangerous output has been or may be executed, the Customer shall:

1. immediately stop subsequent actions or high-risk tasks;
2. take isolation, disconnection, rollback, credential-revocation or credential-rotation measures in accordance with its internal incident process;
3. preserve necessary logs, times, objects, relevant product or device information, instructions and execution results;
4. report the matter through the designated Oneasy support or security channel; and
5. reasonably cooperate with GloryScience in investigation, mitigation and recovery.

7. Prohibited Uses

The Customer shall not use AI Agent Capabilities, or instruct, authorize, assist or knowingly permit another person, to:

1. access, scan, test, control, interfere with or attack any network, device, account, data or credential without authorization, or bypass security controls or obtain unauthorized access to them;
2. generate, distribute or execute malicious code, phishing, fraud, ransomware, denial-of-service activity, credential theft or other unlawful or harmful activity;
3. violate telecommunications regulation, cybersecurity law, communications-secrecy obligations, data-protection law, export controls, sanctions, intellectual-property rights or other applicable law;
4. upload, infer, disclose, associate or re-identify another person's personal data, communications content, trade secrets or other protected information without a lawful basis, necessary authorization or permission under the applicable documents;
5. impersonate another person, or falsify device status, operation records, audit evidence, test results, compliance conclusions, manufacturer opinions, on-site operations or formal authorization;
6. circumvent subscription terms, usage quotas, permissions, billing, logging, auditing, risk controls, content restrictions or other technical or contractual controls;
7. use AI Agent Output as the sole or final basis for a medical, legal, financial, regulatory, contractual, public-safety or other high-impact matter;
8. directly apply AI Agent Output to a High-Risk Network Operation without the required authorization, human review, approval, testing, backup and rollback arrangements;

9. attempt to extract, disclose or bypass Oneasy proprietary system prompts, security rules, model configurations, access controls, tenant isolation or other protective measures;
10. upload, use or request processing of third-party technical materials that the Customer is not entitled to disclose or reproduce, or that are subject to confidentiality obligations or device-manufacturer license restrictions;
11. reverse engineer, decompile, tamper with, bypass, copy without authorization or redistribute Oneasy AI Agent Capabilities, Network Access Components, interfaces, proprietary system prompts or related security controls, except to the extent mandatory applicable law permits or GloryScience expressly authorizes in writing; or
12. misrepresent AI Agent Output, a product name or a compatibility result as an official opinion, certification, endorsement, commitment, quotation, approval, acceptance or authorization issued by GloryScience, Oneasy, a device manufacturer or any third party.

This Section applies cumulatively with the prohibited-use provisions in the Master Agreement and other applicable documents.

8. Human Review, Use of Output and External Publication

Scenario	Minimum Requirement
General Q&A, operating guidance, or a text or table draft	Verify material facts, relevant product and device status, applicable scope and obvious errors before use.
Fault analysis, root-cause inference, device compatibility, configuration, command or script recommendations	Cross-check through personnel familiar with the relevant network, device and on-site conditions; verify official documentation, software or firmware version, logs and actual returned results; and retain unresolved matters as unconfirmed.
Production changes, bulk tasks, remote access or External Execution	Complete the authorization, human review, approval, testing, backup, maintenance-window, execution-confirmation, result-verification and recordkeeping requirements in Section 6.
Security incidents, data breaches, material outages, regulatory or contractual matters	Immediately enter the Customer's designated security, management, legal or compliance process. AI Agent Output shall not replace a formal investigation, decision, notice or report.
External publications, quotations, contracts, reports, audit materials or acceptance materials	Verify facts, sources, rights, authorization and internal approval, and clearly distinguish drafts, recommendations and inferences from formal conclusions.

When using or displaying relevant output externally, the Customer shall not remove, obscure or alter AI identity labels, risk notices or source indicators provided by the product in a manner that is likely to mislead a third party regarding the source, nature or risks of the output.

When quoting or using AI Agent Output, the Customer shall preserve its assisted nature and independently verify cited sources, facts, third-party rights and fitness for purpose. These Rules do not alter the Master Agreement arrangements concerning intellectual property, Customer Content, AI-generated content, feedback or third-party rights.

9. Beta, Trial, Resources and Feature Adjustments

1. AI Agent Capabilities identified as Beta, Preview, Free Trial, Early Access or promotional-period capabilities are provided only within the scope expressly stated in the applicable Order, trial rules, product page, administrative console or written agreement between the parties.
2. Available functions, call volumes, tokens, computing resources, data scope, knowledge bases, models, third-party dependencies and concurrency may be limited by quotas, region, tenant status, risk controls, fair-use requirements and technical conditions.

3. Unless otherwise agreed in an Order, Enterprise SLA or other written agreement, Beta, trial, free or preview capabilities do not create an SLA or a commitment regarding continued availability, performance, functional stability or continued free access.
4. GloryScience may throttle, degrade, suspend, replace, remove or adjust relevant capabilities as reasonably required for security, legal compliance, service stability, abuse prevention, supplier dependency, fair allocation of resources or product iteration.
5. Changes that may have a materially adverse effect on Customer rights are subject to the notice provisions of the Master Agreement, except where immediate action is required for urgent security, legal, regulatory or service-continuity reasons.
6. When GloryScience restricts or suspends a capability, it may, where risk permits and commercially reasonable, limit the measure to what is necessary and reasonably review restoration after the risk has been resolved, the Customer has completed necessary remediation or an alternative control has been confirmed. This paragraph does not create a fixed restoration period or SLA.

10. Support, Incidents, Corrections and Appeals

10.1 Support and Corrections

The Customer shall report issues through the support channels designated in the Oneasy platform, an Order or the official website. These Rules do not establish separate support hours, response times, resolution times or an SLA.

The Customer or an Authorized User may report incorrect output, incorrect refusals, permission issues, data issues, configuration issues or service-use issues, and may request human review or correction. A correction request or appeal does not mean that the relevant output, action, authorization, external publication or business decision has automatically been withdrawn. The Customer must still suspend use, carry out human review, correct external communications and take internal remedial action as appropriate to the nature of the issue.

10.2 Incident Reporting

The Customer shall report the following as soon as reasonably practicable after discovery:

- suspected account or credential compromise, abnormal login or abnormal calls;
- cross-tenant visibility, abnormal permissions or unintended data access;
- dangerous output that has been or may be executed;
- data that has been mistakenly submitted, disclosed, deleted or improperly used in AI Agent processing;
- abnormal remote access, interface use, tool calls or External Execution; or
- another incident that may affect the security of a network, data, a user or the service.

Without disclosing additional sensitive credentials, a report shall, where possible, include tenant information, contact details, time of occurrence, scope of impact, relevant functionality, measures taken and logs, task identifiers or screenshots that may assist an investigation.

The Customer shall promptly take necessary local mitigation measures, including isolation, task termination, credential revocation or rotation, disconnection and rollback, and shall reasonably cooperate with an investigation.

10.3 Risk Measures

Where GloryScience reasonably believes that a security, legal, abuse, data-protection, third-party service, production-network or business-continuity risk exists, GloryScience may suspend, restrict, revoke or degrade the relevant account, AI Agent Capability, API, Network Access Component, remote access or other related functionality in accordance with the Master Agreement and applicable documents.

10.4 Contact Details

- General inquiries and technical support: service@oneasy.cc

- Legal and data-protection matters: legal@oneasy.cc
- Security incidents: the security or support channel designated in the Oneasy platform, an Order or the official website

11. Updates, Acceptance and Effectiveness

11.1 Initial Incorporation and Effectiveness

These Rules become part of the Master Agreement only when they are expressly referenced and accepted by the Customer or its authorized representative through a recordable method. Recordable methods include:

- clicking an acceptance button or selecting a confirmation checkbox;
- express reference and acceptance in an Order, Subscription Order, SOW or other written agreement;
- confirmation in the administrative console or during initial enablement of an AI Agent feature; or
- another method capable of evidencing that the Customer was presented with and accepted the specific text of these Rules.

Merely visiting a webpage that does not expressly incorporate these Rules, storing payment information or using a service unrelated to AI Agent Capabilities does not, by itself, constitute acceptance of these Rules.

11.2 Updates

GloryScience may update these Rules from time to time. A non-material change may take effect by updating the “last updated” date or release notice shown on the official publication page.

For a change that may have a materially adverse effect on Customer rights, GloryScience will follow the notice provisions of the Master Agreement and applicable law. The Customer’s continued use of the applicable AI Agent Capabilities after the notice period expires and the updated text becomes effective constitutes acceptance of the updated Rules.

Where immediate measures are required for urgent security, legal, regulatory, third-party service or service-continuity reasons, GloryScience may first restrict or adjust the relevant capability and provide supplementary notice where reasonably practicable.

11.3 Acceptance Records

For contract administration, audit, security and dispute-handling purposes, GloryScience may record the specific text displayed to the Customer at acceptance or its archived identifier, acceptance time, tenant, administrator or authorized representative, acceptance action and relevant technical records. Such records shall be processed in accordance with the Master Agreement, Privacy Policy, applicable DPA and applicable law.

11.4 Language

If these Rules are available in more than one language, the controlling language is the language specified in the Order, the official publication page or another written agreement between the parties. If no controlling language is specified, the controlling text is the text presented to and retained for the Customer when the Customer completed the acceptance process.

Publisher: GloryScience International Limited

Business Registration Number: 80032746

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

Legal and Data Protection: legal@oneasy.cc

Service Support: service@oneasy.cc