Introduction to KooGallery

Issue 01
Date 2025-01-16

HUAWEI TECHNOLOGIES CO., LTD.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:

https://www.huawei.com/en/psirt/vul-response-process

For vulnerability information, enterprise customers can visit the following web page:

https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Introduction

Huawei Cloud KooGallery is a trustworthy platform for software and service transactions and delivery. In the cloud service ecosystem, KooGallery and its partners are committed to providing customers with high-quality and easy-to-use software, services, and solutions using cloud computing and big data technologies, meeting customer requirements for quick cloud migration and rapid service development.

1.1 Benefits

For Customers

Huawei Cloud KooGallery is dedicated to building an industry-leading platform for application distribution and transaction. **It streamlines application search, purchase, deployment, management, and support. It delivers an efficient, secure, and one-stop shopping experience for businesses.**

1. **Diverse categories**: Shop over 12,000 popular products in 60+ categories, all in one marketplace, to meet your business needs in 10+ common scenarios.

2. **Quick product selection**: Use the smart shopping guide for quick product finding through omni-channel search, recommendations, comparisons, trials, and inquiries. Enjoy up to 180-day product trials before making a decision.

3. **Flexible billing options**: Choose from various billing modes and enjoy exclusive discounts in privates offers from sellers, resellers, or Huawei.

4. **Efficient deployment**: Sign contracts online and deploy software efficiently. Self-service contract management reduces signing duration from months to weeks. Automated deployment also puts you in control, cutting delivery times from weeks to just days.

5. **Security and stability**: Shop with confidence. Our products undergo strict security testing and ongoing vulnerability check and governance. We also have a comprehensive risk management system that safeguards millions of transactions annually.

6. **Professional services**: Get end-to-end, high-quality procurement support services from human agents and automated bots, available 24/7 in over 170 countries and regions.

7. **Shared success**: Leverage KooGallery's open capabilities through Marketplace as a Service (MaaS) to build a dedicated software procurement and management platform.

For Partners

KooGallery provides full-process enablement and support for product distribution and monetization. With powerful and flexible platform capabilities, KooGallery boosts your business growth.

1. **Product release**

    –   Choose from 11 delivery methods and configure details on our user-friendly structured page. Your software products can be listed quickly after a review which takes as little as three working days.

    –   Tap into global markets through a single platform. Just release your products on one website, and we will handle distribution across all sites, including Chinese Mainland website, International website, and local marketplaces.

    –   Pack your products with those of other partners into portfolios, to meet diverse business needs of industry customers and earn more.

2. **Product marketing**

    Leverage Huawei's proven go-to-market capabilities and expertise provided through KooGallery tools and resource, creating more commercial value through shared opportunities.

3. **Continuous operations**

    Analyze your operations and user data on dashboards and secure your operations in KooGallery with flexible settlement capabilities.

1.2 Product Delivery Methods

Huawei Cloud KooGallery provides a platform for partners to release cloud products in various delivery methods, including images, software as a service (SaaS), consulting services, licenses, and professional services. More delivery methods are coming soon.

Images

Images are created by sellers based on the Huawei Cloud public system. Customers can use an image to create an elastic cloud server (ECS) with the same system environment as that in the image.

Images integrate the software environment and functions on the operating system and couple application software with cloud resources to enable out-of-the-box functionality for ECSs.

SaaS

SaaS products are application software products provided by sellers to run on Huawei Cloud infrastructure as a service (IaaS). After purchasing SaaS products,

customers can log in to specified websites to use them without a need to purchase the required cloud resources.

Currently, SaaS products can be enabled by using the username and initial password. When a customer purchases a SaaS product on KooGallery, KooGallery calls the service interface provided by the seller, requesting the seller to perform product subscription. After the subscription operation is complete, the seller returns information to KooGallery, such as the frontend address, management backend address, username, and initial password of the product.

Consulting Services

Consulting services are provided on KooGallery as products. This type of products is not traded on KooGallery. KooGallery only provides links to access the products on sellers' official websites.

Licenses

License products are the licenses of commercial software (such as images and SaaS) provided by a seller. License products include commercial operating system, database middleware, and application software.

Professional Services

Professional services are provided on KooGallery as products and do not involve delivery of software or cloud resources. Such services include environment and configuration, troubleshooting, data migration, consulting, and training.

2 Platform Specifications and Agreements

2.1 Agreements

2.1.1 Seller Agreements

During your use of KooGallery, you need to sign the agreements listed in the following table in different scenarios.

Table 2-1 Seller agreements

Scenario	Agreement	Contracting Parties	Reference
Registering with KooGallery	**[Partner Product] Huawei Cloud KooGallery Partner Product Seller Agreement**	Seller + Huawei Cloud	**Registration**
Joining the joint operations program	**[Joint Operation Product] Huawei Cloud KooGallery Joint Operation Product Seller Agreement**	Seller + Huawei Cloud	**Joint Operations Certification and Product Access**

Viewing a Signed Agreement

Log in to the Seller Console, choose **My Agreements** in the navigation pane, and click **Download** in the row containing an agreement.
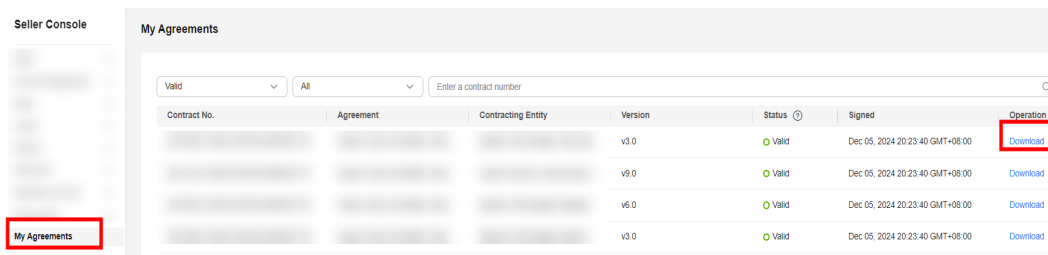
2.1.2 User Agreements

During your use of KooGallery, you need to sign the agreements listed in the following table in different scenarios.

Table 2-2 User agreements

Scenario	Agreement	Contracting Parties
Purchasing a common product	**[Partner Product] Huawei Cloud KooGallery Partner Product User Agreement**	User + Huawei Cloud
	End User License Agreement	User + Seller
Purchasing a joint operations product	**[Joint Operation Product] Huawei Cloud KooGallery Joint Operation Product User Agreement**	User + Huawei Cloud
	End User License Agreement	User + Seller
Purchasing a Huawei proprietary product	**[Huawei Product] Huawei Cloud KooGallery Huawei Product User Agreement**	User + Huawei Cloud
	End User License Agreement	User + Huawei Cloud

☐☐ NOTE

The *End User License Agreement* varies depending on the product. You can click the **Support** tab on the product details page to view the detailed terms.

Viewing a Signed Agreement

Log in to **My KooGallery**, choose **My Agreements** in the navigation pane, and click **View** in the row containing an agreement.
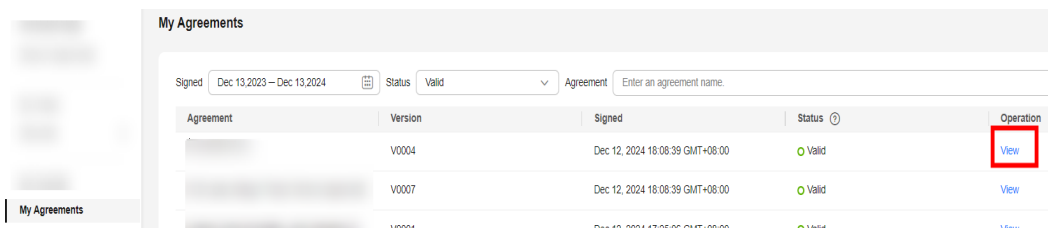
2.2 Specifications

2.2.1 KooGallery Product Security Review Standards 3.0

Sellers are responsible for security vulnerabilities in their released products, including any resulting consequences. The following table lists the specific standards.

Item	KooGallery Product Security Review Standards 3.0
Access control	Isolate users from each other to prevent unauthorized access to resources of other users.
	Limit roles, functions, services, and network ports to the minimum necessary to save space and reduce attack surfaces.
	Provide authentication mechanisms for man-machine interfaces (MMIs) for system management and machine-to-machine (M2M) interfaces across public networks. The interfaces for which standard protocols do not define any access authentication mechanism are excluded.
Security hardening	Before product release, run vulnerability scanning tools. Provide solutions or workarounds for high-risk vulnerabilities (CVSS score 7.0 or higher).
Application security	Check user permission for each access request that requires authorization and perform the final authentication only on the server.
	Use random session IDs for web applications and generate a new session on successful authentication.
Product security	Prohibit functions that allow bypassing system security mechanisms (such as authentication, permission control, and logging) when accessing the system or data.
	Prohibit malware. Before product release, run proven antivirus software to scan for viruses, Trojan horses, or malicious programs.
	Prohibit software with backdoor access.
	Do not run processes that provide services externally or can be remotely accessed as **root** or equivalently authorized accounts.
Encryption	Use open-source-certified algorithms. Use cryptographically secure random numbers in password algorithms.
Data protection	Do not store sensitive data in public object storage buckets or in plaintext. Encrypt such data and control access to it. Sensitive data includes but is not limited to authentication credentials (such as passwords and dynamic tokens), bank accounts, and service keys.

Item	KooGallery Product Security Review Standards 3.0
	Over public networks, transfer sensitive data using secure channels or encrypt it before transmission, unless otherwise specified in standard protocols.
	Do not display authentication credentials in plaintext in logs, debugging information, and error messages stored in the system.
System security	Use system O&M passwords that meet complexity requirements. A password must meet the following requirements: 1. At least eight characters 2. At least two types of the following characters: - Lowercase letters - Uppercase letters - Digits - Spaces and special characters `~!@#$%^&*()-_=+|[{}];:'",<.>/? 3. Different from the account name
	Record management-plane user activities and operation instructions affecting the system in logs to support follow-up audits. Record user ID, time, event type, names of resources accessed, IP address or ID of the client initiating the access, and access result. Control access to logs and prohibit manual deletion or modification of audit logs.
	Prohibit hardcoded passwords (including binary codes and unmodifiable scripts) in software and allow users to change passwords. Upon initial system configuration, forcibly change default passwords of all management accounts that can be accessed externally. Prohibit default permissions from accessing customer running instances.
	Use clear user permission management. New accounts cannot by default be assigned permissions, only a role with the minimum permissions necessary.
Privacy protection	Provide users with a privacy statement before collecting and processing their personal data. The privacy statement covers personal data types, processing purposes, retention period, storage location, and your contact information.
	Obtain user consent before collecting sensitive personal data, such as biometric features, identity information, financial accounts, and usage tracks.
	Collect only the personal data required for service processing. Data types and processing purposes must be as stated in the privacy statement or product documentation.
	Set a retention period of personal data for service processing. Delete or anonymize personal data after this period.

Item	KooGallery Product Security Review Standards 3.0
	Provide a way for users to view, update, export, and delete their personal data.
	Provide security functions (such as authentication, encryption, permissions, and logging) for personal data.
	Obtain separate user consent to share their personal data with a third party. Stop data sharing when users withdraw consent.
	Obtain separate user consent or sign a data transfer agreement with transfer parties for cross-border transfer of personal data.
	Obtain separate user consent and make rejection/withdrawal convenient for using personal data in automatic decisions, personalized recommendations, profiling, and marketing.
Data security	Comply with data security laws and regulations in your country or region throughout the data processing lifecycle. Declare, archive, and report security risks/incidents of important and core data according to Data Security Law of the People's Republic of China.
	Specify your responsibilities and obligations for customer data protection, as well as the purpose, scope, and usage duration, specify the data retention period and clearance method when customers unsubscribe from your services, and promise not to restore the cleared data by technical means in the service statement.
	Specify the legality and authenticity of data sources of any data-related services you provide in the service statement.
	Take security measures for Huawei Cloud and customers' data assets to prevent disclosure due to improper protection.
	Do not use the data provided by Huawei Cloud beyond the purpose, scope, and period authorized by Huawei Cloud. Do not provide data related to Huawei Cloud to third parties.
	If a data security incident, such as data breach, damage, and ransomware, occurs due to your reasons, take remedial measures immediately after detecting the incident, report the incident information and result according to regulatory requirements, and notify Huawei Cloud.
Integrity protection	Encrypt software/patches or use secure delivery to customers. Provide integrity verification such as hashing.
Lifecycle management	Do not use platforms, open-source components, or third-party components that reach End-of-Life (EOL) in the product.

Item	KooGallery Product Security Review Standards 3.0
O&M security	Do not use preset, empty, or weak passwords for interfaces connected to the public network. Unless there are industry-compliant input restrictions, passwords must meet the following requirements: 1. At least eight characters 2. At least two types of the following characters: - Lowercase letters - Uppercase letters - Digits - Spaces and special characters `~!@#$%^&*()-_=+|[{}];:'",<.>/? 3. Different from the account name Display a warning message for invalid passwords.
	Comply with the *Huawei Cloud KooGallery Partner Product Seller Agreement* for vulnerability notification and fixing.
	Do not open high-risk services to the public network. If this is unavoidable, take peripheral network security measures and describe them in the product documentation.

2.3 Notices

2.3.1 Notice on Updating the Platform Fee Rule of Common Products

Dear KooGallery sellers:

From January 01, 2025, KooGallery will charge a 10% platform fee on common product transactions, regardless of the product delivery method.