Huawei Cloud Cyber Security and Privacy Protection FAQs

Issue	**1.2**
Date	**2024-08-08**

Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Security and Privacy Governance

1.1 Strategy and Planning

1.1.1 What are the objectives of or principles behind Huawei Cloud cyber security and privacy protection?

Cyber security objectives and principles: Huawei Cloud takes data protection extremely seriously. Security technologies are foundational. Compliance with applicable cyber security laws, regulations, and industry standards are the castle walls that protect us, and the wider security ecosystem is our moat. Huawei has leveraged unique software and hardware advantages to establish and maintain industry leadership and competitiveness with well-managed cloud security infrastructure and services. They protect Huawei Cloud services across regions and industries. This commitment to security is a key strategy for Huawei Cloud.

Privacy protection objective and principle: Huawei Cloud shall adhere to neutrality, strictly abide by the service boundaries, and ensure that data is owned and used by and for customers. Huawei Cloud commits that it will comply with applicable privacy laws and regulations in the countries or regions where it operates.

1.1.2 How are Huawei Cloud cyber security and privacy organizations organized?

By unswervingly building cyber security and privacy protection capabilities in products and services, Huawei cloud build competitiveness from the inside out and comply with applicable cyber security and privacy protection laws and regulations. Huawei cloud places its responsibility for network and service security above the company's business interests and continuously creates value for customers. In terms of organization, the Board of Directors (BOD) /Executive Management Team (EMT), as the highest cyber security and privacy protection management organization, is responsible for approving corporate cyber security and privacy protection governance solutions, policies, and strategies. The Global Cyber Security and Privacy Protection Office (GSPO) develops cyber security strategies and builds a cyber security assurance system. The GSPO directly reports to the EMT/BOD.

While upholding Huawei's cyber security strategy and standards, the Huawei Cloud security team enjoys autonomy in its security planning and management activities. Huawei Cloud combines its R&D and operation & maintenance (O&M) business functions for cloud services and cloud security services. The organizational structure is flat by design, accommodating the DevOps and DevSecOps processes best suited for cloud services. This flat organizational structure and the cloud service–oriented processes it covers befit rapid, continuous integration, delivery, and deployment of cloud services. They also ensure that cloud services

meet the necessary security standards and can effectively manage risks. Through processes such as cloud security engineering, cloud service and solution design and development, and O&M, Huawei Cloud has developed its own service security compliance and security O&M. This system effectively protects the interests of Huawei Cloud customers. Due to the unique importance of cloud security to Huawei Cloud, the cloud security team reports directly to the president of Huawei Cloud. HUAWEI CLOUD sets up Regional Cyber Security Officers (CSO) in each region/key country to communicate with local governments and customers and ensure that local compliance requirements are met.

1.2 Risk Management

1.2.1 What are your risk management processes like?

Cloud security governance can be broken down into multiple processes. Each process has corresponding inputs, controls, and outputs. As compliance has been getting prioritized more and more lately on the international market, compliance is a top-of-mind issue for both cloud service providers and customers alike. This extra focus on compliance makes it easier to understand and promptly respond to dynamic changes in cloud security governance requirements. Properly managing risks to cloud assets and cloud services is also critical. Currently, most mainstream risk management approaches are based on assets and threats. The objects of Huawei Cloud security governance are similar to those considered in other authoritative standards. In Huawei Cloud security governance framework, the core inputs for controls mainly consist of security compliance requirements and security risks.

1.2.2 What laws and regulations does Huawei Cloud comply with?

Huawei Cloud not only adopts the industry's best security practices, but also complies with applicable security policies and regulations in the countries or regions where it operates, as well as international cyber security and cloud security standards. This forms our security baseline. Huawei Cloud has established and is always improving upon security-related organizations, processes, and standards, as well as technical capabilities, compliance, and ecosystem construction. Our aim is to provide you with highly trustworthy and sustainable security infrastructure and services. We also openly and cooperatively address cloud security challenges with our customers and partners, as well as the relevant governments, to meet the security requirements of our cloud users.

1.2.3 What are the compliance responsibilities of Huawei Cloud? Do I have any compliance responsibilities?

Huawei Cloud is committed to providing you with secure and compliant infrastructure and services, with each service having built-in security functions. We provide continuous O&M to ensure the security of our services. We ensure that all our infrastructure and services provided for you are assessed and have passed review by authoritative independent third-party organizations and security certification bodies.

When using Huawei Cloud services, you need to consider the security and compliance of your internal applications and any customized configurations based on the features of the cloud services you use. You are the owners and controllers of your data. Therefore, you are responsible for specific data security configurations, data confidentiality, integrity, and availability (CIA), and identity authentication and authorization for data access. In addition, you

should ensure that the services meet corresponding regulatory requirements based on service features.

For more details about the security responsibilities, see the *Huawei Cloud Security White Paper*.

1.3 Privacy Protection

1.3.1 What personal data will be collected by Huawei Cloud platform and for what purposes? Where can I obtain the privacy statement?

During your interaction with Huawei Cloud, Huawei Cloud collects your personal data only when necessary, such as for providing services for you. We collect your personal data in the following scenarios:

- When you use a Huawei ID, we collect your username, mobile number, email address, and account information.
- When you use the address management service, we collect your recipient name, detailed address, postal code, and mobile number.

For more scenarios, see the Privacy Statement.

Privacy Statement: https://www.huaweicloud.com/intl/en-us/declaration-sg/sa_prp.html

Huawei Cloud respects and protects your personal data in accordance with the Privacy Statement. Huawei Cloud collects, stores, and uses your personal data in compliance with the principle of data minimization, and takes comprehensive measures to secure such data.

1.3.2 How does Huawei Cloud platform ensure legitimate collection and processing of my personal data?

The Privacy Statement of Huawei Cloud describes for what purposes and how we will collect and process your personal data. Huawei Cloud shares or discloses your personal data to a third party only within the scope permitted by applicable laws and regulations in accordance with the Privacy Statement. After obtaining your explicit consent, we will share the authorized data with the third party designated by you. We may disclose your personal data to our affiliates so that they can provide transaction, service, or security support for you.

Privacy Statement: https://www.huaweicloud.com/intl/en-us/declaration-sg/sa_prp.html

1.3.3 How can I access or control my personal data?

You need to ensure that any personal data you provide is correct and accurate. We will try our best to maintain the accuracy and integrity of the data and update such data promptly based on any more recent data you provide.

You can access and modify the personal data we hold about you in the following ways:

- **Account information:**

To add or update personal data related to your accounts, you can go to the Huawei Cloud International website, click **Log In** and enter your account information. On the displayed page, click **My Account** to modify data as needed.

- **Cookies:**

To learn more about how cookies are managed, see the Cookie Policy.

Cookie Policy: https://www.huaweicloud.com/intl/zh-cn/declaration/sa_cookies.html

- **Message:**

To modify information related to messages, you can go to the Huawei Cloud International website, click **Log in**, and enter your account information. On the upper right corner of the displayed page, click the Email icon to view unread messages. After clicking the Email icon, you can also configure **Message Receive Management**.

For more details about how you can access and control your personal data, please see the Privacy Statement.

Privacy Statement: https://www.huaweicloud.com/intl/en-us/declaration-sg/sa_prp.html

1.3.4 Will my data be transferred across borders for remote O&M, and what data will be transferred across borders?

Huawei Cloud has data centers in several countries around the world. If cross-border data transfer is needed for purposes such as O&M, Huawei Cloud will comply with local privacy laws and regulations and strictly review the transfer. Huawei Cloud will transfer personal data across borders only after, for example, a data transfer agreement is signed, or your explicit consent is obtained. This is to ensure that your personal data is processed lawfully, fairly, and transparently. For more details, please see the Privacy Statement.

Privacy Statement: https://www.huaweicloud.com/intl/en-us/declaration-sg/sa_prp.html

For remote O&M, the following categories of data may be transferred across borders to the O&M center:

Log data: includes system logs, access logs, and service run logs of hosts and VMs.

Indicator data: includes monitoring data reported by system indicators (such as the CPU and memory), service indicator, and tenant monitoring indicators (such as the CPU, memory, and number of connections of hosts and VMs) services.

1.3.5 How does Huawei Cloud protect my account information?

Huawei Cloud respects and protects your account information in accordance with its Privacy Statement. Huawei Cloud collects, stores, and uses your account information in compliance with the principle of data minimization, and takes comprehensive measures to secure your account information.

1.3.6 How does Huawei Cloud secure my personal data when providing support services?

We place great importance on the security of your personal data. We take all appropriate physical, management, and technical measures to protect your personal data.

For example, we use encryption to ensure data confidentiality; use trustworthy protection mechanisms to defend against data attacks; deploy access control mechanisms to ensure that only authorized personnel can access personal data; and we raise awareness among our employees about the importance of protecting personal data through security and privacy protection training sessions.

We also incorporate management measures of personal data protection into the personal data processing lifecycle. For more details, please see our Personal Data Protection Practices.

Personal Data Protection Practices: https://www.huaweicloud.com/intl/en-us/securecenter/privacy/personal-data-protection.html

1.3.7 Will my personal data be retained after I have deregistered my cloud account?

After you deregister your account, we will keep your registration details for a period of time for problem tracing and auditing before deleting them. The period of time is determined by applicable laws and regulations.

1.3.8 What privacy protection certifications has Huawei Cloud earned?

So far, Huawei Cloud has earned many certifications, such as ISO 27018, ISO 27701, BS 10012, ISO 29151, and ISO 27799. We comply with related privacy standards in terms of data processing, storage, categorization, and classification. For more details, please go to our Compliance Center.

Compliance Center: https://www.huaweicloud.com/intl/en-us/securecenter/compliance/compliance-center.html

1.3.9 Does Huawei Cloud comply with the GDPR?

The cyber security and privacy protection framework of Huawei Cloud has incorporated privacy protection laws and regulations of multiple countries around the world. In addition to the GDPR, Huawei Cloud also refers to privacy protection laws and regulations of major European countries, such as Ireland, Spain, and Switzerland, to enhance the privacy protection capabilities of our platform, with the aim of protecting the privacy rights of EU citizens. Huawei Cloud conducts regular internal and external reviews to ensure that services we provide comply with local laws, regulations, and industry standards.

So far, we have earned many certifications, including ISO 27018, ISO 27701, BS 10012, ISO 29151, and ISO 27799. We comply with related privacy standards in terms of data processing, storage, categorization, and classification.

1.3.10 Which channels are used by the Huawei Cloud platform to respond to my requests for exercising my data subject rights regarding personal data?

Huawei Cloud provides different channels for you to make requests and has a professional team to process these requests. The team quickly responds to and processes the received requests, and notifies you of the results.

If you have any questions, comments, or suggestions, you can contact us via the customer service hotline. You can also make requests on the **Personal Data Management Request** page.

Personal Data Management Request page: https://www.huawei.com/en/personal-data-request

1.3.11 How does Huawei Cloud handle data breaches?

To minimize the impact of personal data breaches, Huawei Cloud has developed a process to manage these events. In addition, we have a dedicated privacy protection team, which promptly discloses personal data breaches in line with applicable laws and regulations, and implements emergency plans and recovery processes to minimize impacts. Huawei Cloud provides multiple channels for reporting personal data breaches, ensuring that relevant owners are notified of the breaches as soon as possible. In the early stages of a personal data breach, related teams will take necessary technical measures based on the emergency plan to prevent aggravating the impacts on you. If the breach needs to be reported to external organizations (including regulators and customers) or affected data subjects according to local laws, regulations, or contracts, dedicated persons will report a breach using a specified template.

1.3.12 If I have questions about personal data protection, who should I contact?

Huawei Cloud has a department dedicated to personal data protection to help resolve your questions about personal data protection. If you have any questions, comments, or suggestions, you can contact us via the customer service hotline or via the **Personal Data Management Request** page.

Personal Data Management Request page: https://www.huawei.com/en/personal-data-request

1.4 Data Security

1.4.1 What are the rules of Huawei Cloud for categorizing and classifying data?

Huawei Cloud assesses four aspects of data security: confidentiality, integrity, availability, and compliance. We assess impacts of a breach, damage to stored data, or other compromises on Huawei Cloud based on these four categories.

1.4.2 What are the common categories of my data?

When providing services, Huawei Cloud generally processes two types of your data:

- **Personal data:**

Personal data is any data that, either on its own or together with other data, can be used to identify a natural person. During your interaction with Huawei Cloud, Huawei Cloud collects your personal data for necessary purposes only, such as for providing services for you. We collect your personal data in the following scenarios: When you use a Huawei ID, we collect your username, mobile number, email address, and account information; when you use the address management service, we collect your recipient names, addresses, postal code, and mobile number. For more scenarios, see the Privacy Statement.

Privacy Statement: https://www.huaweicloud.com/intl/en-us/declaration-sg/sa_prp.html

Huawei Cloud respects and protects your personal data in accordance with the Privacy Statement. Huawei Cloud collects, stores, and uses your personal data in compliance with the principle of data minimization, and takes comprehensive measures to secure such data.

- **Content data:**

Content data refers to data stored or processed during the use of Huawei Cloud services, including but not limited to documents, software data, images, and audio and video files.

You own and control your content data and are responsible for security of such data. We provide a diverse range of services for you to choose from. We will do everything we can to help you improve security and minimize data security risks.

1.4.3 Who decides where my content is stored?

You decide where the data is stored. Huawei Cloud provides services in different regions, and you can choose which region your data is stored in. Without authorization, Huawei Cloud never moves your data across regions. When using Huawei Cloud services, you are advised to select regions to store your content near where the data will be accessed, but also in accordance with the laws and regulations of different regions.

1.4.4 Where will my content data be stored?

Huawei Cloud regions and availability zones (AZs) are deployed around the world and offer high-speed global network connections and localized services. You can select a Huawei Cloud region to purchase and deploy services as needed. The region selected is where your content will be stored. Without your authorization, Huawei Cloud will never move your content across regions. For example, if you purchase services in the Singapore region, your data will be stored only in Singapore.

For more information about Huawei Cloud regions and AZs, please see the global infrastructure distribution on the Huawei Cloud International website.

Huawei Cloud International website: https://www.huaweicloud.com/intl/en-us/

1.4.5 Does Huawei Cloud transfer my data to other regions or countries?

Content data: You can decide what region your content data is stored in. Huawei Cloud will never transfer your content data to other regions without your explicit consent or unless required by law. If you intend to transfer your data across borders and need assistance from Huawei Cloud, you can contact and authorize us to transfer the data.

Personal data: Huawei Cloud provides products and services through our global resources and servers. Any personal data we collect may be stored in countries or regions where Huawei Cloud, its affiliates, service providers, and subcontractors are located. This means that your personal data may be transferred to other jurisdictions outside the country or region where the product or service is used, or may be accessed from these jurisdictions. Laws protecting personal data vary by jurisdiction. Different jurisdictions may have laws protecting personal information to varying degrees or may not have personal data protection laws at all. Huawei Cloud ensures that your personal data is protected in compliance with applicable laws, regulations, and the Privacy Statement. For details, see question 1.3.4 "Will my data be transferred across borders for remote O&M, and what data will be transferred across borders?"

Personal data of customers in the Chinese mainland will be stored on servers in the Chinese mainland.

1.4.6 What capabilities does Huawei Cloud provide to ensure the security of my data?

Huawei Cloud establishes and runs a complete, highly trustworthy, and sustainable data security governance system from perspectives of organizational responsibilities, policy requirements, process guidance, technical tools, and measurement and verification in compliance with legal and regulatory requirements, international and industry data security standards, as well as industry best practices. This system effectively ensures the security of your data.

At the technical level, Huawei Cloud offers a range of services to ensure data security, for example, the Data Security Center (DSC), Data Encryption Workshop (DEW), Database Security Service (DBSS), Cloud Eye Service (CES), Log Tank Service (LTS), Cloud Trace Service (CTS), Web Application Firewall (WAF), and anti-DDoS service. Among them, the CES is a multi-dimensional platform for monitoring elastic cloud servers, bandwidth, and other resources. The LTS allows you to collect and store logs and query them in real time, making routine O&M easier, such as real-time collection of logs, query, and analysis. The CTS provides records of operations on cloud service resources. With the CTS, you can query, audit, and backtrack operations. The WAF has a dual-engine architecture based on regular expressions and semantic analysis to ensure high-performance protection against SQL injections, Cross-Site Scripting (XSS) attacks, command and code injections, directory traversals, scanners, malicious bots, and other attacks. The anti-DDoS service uses sophisticated anti-DDoS devices to accurately and effectively defend against traffic attacks and application-layer attacks.

1.4.7 How does Huawei Cloud protect data when transmitting it on the public network?

When data is transmitted between servers and clients of Huawei Cloud and between servers of Huawei Cloud through public channels, the data is protected by a virtual private network (VPN) as well as application-layer Transport Layer Security (TLS) and certificate management. Huawei Cloud not only ensures the security of data transmission on the cloud, but also provides you with high-performance, high-reliability, and low-latency network transmission. Huawei Cloud provides multi-link disaster recovery (DR) by allowing you to access your Virtual Private Clouds (VPCs) on the cloud via multiple dedicated connections from different carriers. If one link fails, or the entire network of a carrier fails, traffic automatically fails over to another link provided by another carrier, ensuring service continuity.

1.4.8 How does the Huawei Cloud platform ensure the security of my data?

We understand that your data assets are extremely valuable and consider data protection the core of our security policies. We comply with industry-leading standards on data security lifecycle management. We use excellent technologies, practices, and processes for identity authentication, permissions management, access control, data isolation, transmission security, storage security, data deletion, physical destruction, and more. For details, see the *Huawei Cloud Data Security White Paper*.

Huawei Cloud Data Security White Paper: https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/Best%20Practices/DataSecurityWhitepaper_intl_en.pdf

It is worth emphasizing that you own all of the content data generated when you use Huawei Cloud services. You have full control over your data, but you are also responsible for configuring security measures for specific data and ensuring the confidentiality, integrity,

availability, and data access authentication. For example, when using Identity and Access Management (IAM) and Data Encryption Workshop (DEW) services, you are responsible for keeping your service accounts, passwords, and keys safe, and you should comply with industry best practices in configuring, updating, and resetting passwords and keys. For more data security products, see the **Security & Compliance** section at the **All Products** page.

All Products page: https://www.huaweicloud.com/intl/en-us/product/

1.4.9 Will Huawei Cloud access my content data?

As a cloud infrastructure and service provider, we understand your concerns about data security. We always comply with local laws and regulations on data security. Without your explicit consent, we will never use, or even access, your non-public content data.

1.4.10 When I delete content data stored in Huawei Cloud services, is it deleted from Huawei Cloud immediately?

When you delete content data stored in a Huawei Cloud service, the service will delete the data immediately. However, some services that provide a recycle bin or other function to protect your data from accidental deletion. These features will retain the data for a certain period of time. For more details, see the user guide of related services on the Huawei Cloud website. You can search for keywords such as Recycle Bin and Data Destruction on the Huawei Cloud website to view the data deletion retention periods specified for different services.

1.4.11 Will my content data be deleted immediately if my subscription to a service expires or my account falls into arrears?

If yearly/monthly resources expire or not renewed due to payment failures, we provide a grace period for you to renew the resources or to pay off the outstanding orders. During this period, you can continue to access and use some resources. A 15-day grace period is provided on the Huawei Cloud International and European websites. For details, visit: https://support.huaweicloud.com/intl/en-us/faq-billing/postRules_topic_100014.html

1.4.12 Will my content data be deleted immediately when I delete my Huawei Cloud account?

Before deleting an account, you need to close the account. After the account is closed, the account enters the retention period, and the data stored in Huawei Cloud will be deleted and cannot be restored. However, there may be a retention period for some services, which is explicitly described in the corresponding user guide. During this period, you can still use your account to log in to Huawei Cloud and view the account and expenditure details. After the retention period expires, your account will be automatically deleted and can no longer be used. For details, see: https://support.huaweicloud.com/intl/en-us/usermanual-account/en-us_topic_0149890045.html

1.5 Awareness & Education

1.5.1 How is your employees' participation in cyber security awareness training? Where can I see the evidence of training?

Our employees are required to take part in a range of training sessions at many stages, such as during onboarding, while on the job, and upon a job promotion. This is to ensure that they act in compliance with the security standards of Huawei Cloud.

2 Security and Privacy Verification and Communication

2.1 Assessment/Inspection/Measurement by the Red Team

2.1.1 How does Huawei test the security of the Huawei Cloud platform?

Huawei Cloud's security operations team uses vulnerability scanning, penetration testing, and other security tests on the Huawei Cloud platform to ensure security.

2.1.2 How are users notified of vulnerabilities on the Huawei Cloud platform?

To protect users, Huawei Cloud is committed to responsible vulnerability disclosure. For vulnerabilities related to the cloud platform and tenant services, Huawei Cloud reports vulnerability mitigation and remediation solutions and suggestions to users in a timely manner while ensuring that the proactive disclosure will not cause higher risks of attacks. We work with users to address the challenges of any security vulnerabilities that have been discovered.

2.1.3 What are the threat and vulnerability management processes of the Huawei Cloud platform?

Huawei Cloud has a mature threat and vulnerability management process to quickly locate and resolve threats and vulnerabilities, reducing the impact on tenant services.

2.1.4 What are Huawei Cloud's requirements, processes, and execution of assessments and audits?

Huawei Cloud undergoes strict audits, which play a key role in promoting cyber security processes and standards. Huawei has a dedicated security audit team that audits Huawei Cloud once a year. They focus on risks related to Huawei Cloud legal and process compliance, business objectives, reliability of decision-making information, and security O&M, and they ensure that audit findings are rectified.

2.1.5 How does Huawei Cloud meet requirements for remediating vulnerabilities within a certain period of time?

Huawei Cloud has access to comprehensive network configuration details and device permissions. Huawei Cloud has adopted the DevOps/DevSecOps process to support rapid and direct continuous integration and deployment in the vulnerability remediation process. Huawei Cloud has an end-to-end vulnerability response service ticket system for everything from vulnerability awareness to live-network remediation. This system automatically receives vulnerability information from multiple channels, such as the Huawei Product Security Incident Response Team (PSIRT) and various online scanning tools. It automatically assigns handling priorities based on the severities of the vulnerabilities, and it then specifies the remediation Service Level Agreement (SLA).

2.2 External Communication

2.2.1 How does Huawei Cloud notify users of personal data breaches?

When a personal data breach occurs, Huawei Cloud reports the breach based on national regulations and internal processes in line with Huawei's transparency principle.

2.2.2 Where can I obtain cyber security and privacy protection white papers?

White papers related to cyber security and privacy protection can be obtained from the Trust Center of Huawei Cloud. Related resources are shown below.

International sites of Huawei Cloud:

- Trust Center: https://www.huaweicloud.com/intl/en-us/securecenter/overallsafety
- White Paper for Huawei Cloud Trustworthiness: https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/Best%20Practices/Trustworthiness_Whitepaper_intl_en.pdf
- Huawei Cloud Privacy Protection White Paper: https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/Best%20Practices/Privacy_Protection_intl_en.pdf
- Huawei Cloud Security White Paper: https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/Best%20Practices/SecurityWhitepaper_intl_en.pdf
- Huawei Cloud Data Security White Paper: https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/Best%20Practices/DataSecurityWhitepaper_intl_en.pdf

2.3 Certification and Audit

2.3.1 What security/privacy certifications does Huawei Cloud have?

Huawei Cloud is committed to providing secure and trusted cloud services. The infrastructure and services provided by Huawei Cloud have been reviewed and approved by independent

third-party authorities recognized throughout the industry and have earned security certification from numerous organizations.

Huawei Cloud has been certificated by various international authorities and is compliant with industry standards. Examples include:

Security standards: ISO 27001, ISO 27017, CSA STAR gold certification, DJCP (Classified Protection) level 3 and 4 by China's Ministry of Public Security (MPS), PCI DSS for the payment card industry, and NIST Cybersecurity Framework (CSF)

Privacy standards: ISO 27018, ISO 27701, BS 10012, ISO 29151, and ISO 27799

More certification information is available on the **Compliance Certificates** tab page of the Compliance Center.

In addition to the third-party certifications, you can find solutions to compliance issues on the **Country/Region-specific Guidance** and **Industry-specific Guidance** pages of the Compliance Center of Huawei Cloud.

Compliance Center: https://www.huaweicloud.com/intl/en-us/securecenter/compliance

2.3.2 Can I download a copy of these certificates?

Yes. You can download certificates from the Trust Center. If you want to know what the certificates cover, or if you need assistance from Huawei Cloud when your business is being certified, you can apply for and download a copy of the certificates in the **Download Compliance Certificates** area of the Compliance Center of Huawei Cloud.

Compliance Center: https://www.huaweicloud.com/intl/en-us/securecenter/compliance

2.3.3 What audit reports does Huawei Cloud provide?

Huawei Cloud has released SOC 1/2/3 reports and Outsourced Service Provider Audit Report (OSPAR). You can obtain the reports from the Compliance Center of Huawei Cloud.

Compliance Center: https://www.huaweicloud.com/intl/en-us/securecenter/compliance

2.3.4 What compliance services does Huawei Cloud provide to help me get certified faster?

Huawei Cloud keeps an eye on changes of laws and regulations and develops security services and one-stop security solutions based on its extensive experience to help you comply with the business security requirements and quickly obtain required certificates. Take the Database Security Service (DBSS) as an example. It complies with the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and PCI DSS, so it meets audit requirements. You can use it to audit the important behavior and security events of every user. In addition, DBSS provides compliance reports that meet data security standards (such as SOX).

2.3.5 What third-party audit evidence does the Huawei Cloud platform use to prove compliance with security best practices?

Huawei Cloud has obtained authoritative certifications and audit reports, such as SOC 1/2/3 reports, ISO 27001, ISO 27017, ISO 27018, and CSA STAR gold certifications, as a testimony of its compliance with industry best practices. In addition, Huawei Cloud optimizes security control requirements and methods based on compliance requirements and industry standards

in different regions around the world, such as Multi-Tier Cloud Security (MTCS) Level 3 in Singapore and trusted cloud in China.

2.3.6 What regions and cloud platform services does each certification of Huawei Cloud cover?

Huawei Cloud has earned security certifications for all its regions, AZs, and more than 140 cloud services. It has earned regional certifications, such as MTCS, for all the local regions, AZs, and cloud services. You can view the certified services from the Compliance Center of Huawei Cloud.

Compliance Center: https://www.huaweicloud.com/intl/en-us/securecenter/compliance

2.3.7 What government-level security certifications has Huawei Cloud obtained? Which sectors are these certifications applicable to?

Huawei Cloud has obtained security certifications for sectors such as credit card, health, finance, automobile, and government. Government-level security certifications include DJCP (Classified Protection) by the Chinese government, cyber security review by the Cyberspace Administration of China, and MTCS Level 3 certification by the Singapore government. In addition, Huawei Cloud has released multiple compliance white papers adapted to laws and regulations around the world, including Brazil, Malaysia, and Singapore. For details, visit the Compliance Center of Huawei Cloud.

Compliance Center: https://www.huaweicloud.com/intl/en-us/securecenter/compliance

2.3.8 How does Huawei Cloud maintain related certifications?

Huawei Cloud certifications are reviewed and updated annually based on certification requirements.

2.3.9 What services does Huawei Cloud offer to help me earn cloud-related certifications?

Huawei Cloud customer service personnel are ready to help when you need support from Huawei Cloud during certifications.

3 Service/Solution Security and Privacy Compliance

3.1 Supply Chain Security

3.1.1 Where can I obtain a list of Huawei Cloud suppliers (including suppliers of data centers, software, and hardware)?

For business security reasons, a supplier list cannot be provided. Suppliers entrusted by Huawei Cloud to process personal data include suppliers of commodities or technologies, advertisement, survey, analysis, and return visit services. In addition, Huawei Cloud may share personal data with business partners, including independent software or service providers in the KooGallery. The entrusted processing and sharing of personal data with third parties have been disclosed in the Service Agreement.

Service Agreement: https://www.huaweicloud.com/intl/en-us/declaration/tsa_ssl

3.1.2 What are Huawei Cloud's cyber security requirements and how are suppliers supervised and reviewed?

Huawei Cloud has requirements for supplier supervision based on our own cyber security and privacy requirements. Huawei Cloud evaluates supplier qualifications before procurement and only procures from qualified suppliers. Huawei Cloud signs a contract, service agreement, and a non-disclosure agreement with candidate suppliers to specify responsibilities, obligations, and service level requirements before introducing them. After a supplier is introduced, Huawei Cloud conducts supplier security system inspection. We examine the supplier's security agreement execution, capabilities, and closed-loop management of issues, covering the supplier's security organizations, security R&D tests, vulnerability management, and other aspects.

3.2 Development and Deployment Security

3.2.1 How does Huawei Cloud ensure products comply with security and privacy protection requirements?

Huawei Cloud has considered security and privacy protection requirements in the product design phase. Huawei Cloud has a system of eight principles of trustworthy service design that we strictly comply with. Security policies are formulated during product design. During development, Huawei's internal requirements for cyber security restricted features are followed to ensure that related restricted features are approved by specific departments, and code is compiled using preferred compilers according to secure coding specifications. After development is complete, only the recommended tools are used to inspect the code.

3.2.2 How is code security ensured during development?

During development, Huawei Cloud follows internal requirements for cyber security restricted features. We ensure that related restricted features are reviewed by specific departments, and compile code using preferred compilers according to secure coding specifications. After the development is complete, we use static code scanning tools to inspect the code and analyze alarms. High-risk alarms and must-be-cleared alarms are all cleared.

3.2.3 How does Huawei Cloud ensure that vulnerabilities or backdoors are detected in a timely manner during development?

All cloud services have passed multiple rounds of security tests and reviews before being released, including but not limited to microservice-level functions (such as authentication and session security) and interface security tests in the Alpha phase. Test cases cover security requirements identified in the security design phase and penetration testing cases.

3.2.4 Where does the test data come from? Will customer data be used for testing and AI training?

Using production environment data in the development and testing environments is generally prohibited. If it is absolutely necessary to do so, authentication credentials and confidential business data must be filtered out from the production data before the production data can be used for development or testing, and personal data in the production data must be anonymized while compliance is ensured. Huawei Cloud adheres to data neutrality and never accesses or uses customer data without authorization.

3.3 Delivery and O&M Security

3.3.1 Which Huawei Cloud services can help me comply with security regulations?

Huawei Cloud is committed to ensuring the security of IaaS, PaaS, and SaaS cloud services and infrastructure, and providing advanced, stable, reliable, and secure products and services. You can refer to the **Security Features** page to configure Huawei Cloud services for security compliance.

Security Features: https://www.huaweicloud.com/intl/en-us/securecenter/security/security_features

3.3.2 How does Huawei Cloud ensure that unauthorized internal personnel and O&M personnel cannot access tenant data?

The management zone and tenant resource zone of Huawei Cloud are at different network planes. Huawei Cloud isolated resources to keep them secure. The CPU, memory, and I/O on the tenant plane are all kept isolated from the management plane. Huawei Cloud strictly controls access to the platform and what operations can be performed on the platform. Only authorized personnel can access the production environment during the authorized period. In addition, any major changes on the live network can be implemented only after being approved. Huawei Cloud also has a comprehensive O&M audit system. All O&M operations performed by internal personnel are recorded. Huawei Cloud regularly monitors and audits activities in the O&M process, and generates alarms for and terminates abnormal operations in a timely manner. Any violations of O&M regulations are punished in accordance with relevant corporate regulations. Huawei Cloud promises that it will never access tenant content data without authorization.

3.3.3 How are security and privacy risks managed during change implementations?

Huawei Cloud will analyze the risks of all changes and implement different risk controls based on the analysis results to protect security and privacy when changes are implemented.

3.3.4 When do tenants need to be notified during change implementations?

Huawei Cloud has established a mature change mechanism and process. Changes are classified into four levels based on their impact on customers. For changes that may cause the unavailability of Huawei Cloud systems or customer services, or failures of major IT infrastructure, the Huawei Cloud Change Approval Committee reviews the cyber security and privacy risks of the change solution and provides related information to relevant cloud customers by means of calls, SMS messages, bulletins on the official website, or others.

3.3.5 What is the access control policy (account, permission, and password management mechanism) of Huawei Cloud's O&M platform?

When managing system permissions, the O&M entity of Huawei Cloud enforces separation of duties (SOD), work relevance, proper authorization, and controlled approval to ensure the principle of least privilege. Our password policy is also in line with industry standards.

3.3.6 How are accounts and permissions kept up to date?

Huawei Cloud has a regular permissions review system. User permissions are reviewed once a month for the O&M management platform and once a quarter for the operations account center. If any exceptions are found, the responsible department follows up and updates account permissions as needed. When an employee resigns or is transferred to another position, the account held by the employee is deleted within a specified period of time.

3.3.7 How are logs collected and stored and how are security incidents monitored, analyzed, and responded to?

Huawei Cloud uses a log big data analysis system to quickly collect, process, and analyze logs in real time. It can connect to Security Information and Event Management (SIEM) systems provided by third parties, such as ArcSight and Splunk.

3.3.8 What logs are collected by Huawei Cloud's security management platform? Do the logs ever include customer data?

The security management platform collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems to monitor related performance indicators and ensure that the underlying devices of tenants are running properly. The security logs of Huawei Cloud do not contain sensitive personal data. If logs need to contain personal data that is directly related to network security threats, the data is encrypted or anonymized as appropriate.

3.3.9 What practices or products does Huawei Cloud use during O&M?

In DevOps or DevSecOps, O&M is as important as R&D. Huawei Cloud takes O&M very seriously and has numerous established practices for O&M security, vulnerability management, security event management, service continuity, and disaster recovery management. Take O&M access as an example. Huawei Cloud uses VPNs and Cloud Bastion Hosts deployed in your data center to manage and audit your server O&M in a unified manner, and takes different security control measures for different operations. For more information, see "Operational Security" in *Huawei Cloud Security White Paper*.

You can also learn about secure and intelligent O&M from Huawei Cloud courses. For details about services recommended for O&M security, go to the **Operation and Maintenance Security** page.

Operation and Maintenance Security: https://www.huaweicloud.com/intl/en-us/securecenter/security/operationsafety

3.3.10 What is the vulnerability management policy of Huawei Cloud? How does Huawei ensure timely vulnerability remediation and patch installation?

Huawei Cloud has established multiple channels for collecting vulnerability information. Its vulnerability management mechanism is updated every year. In addition, it uses automatic vulnerability scanning tools to scan boundary vulnerabilities 24 hours a day, 7 days a week and scan vulnerabilities on the internal management plane every month. It develops a vulnerability remediation plan and deadline for each discovered vulnerability based on the SLA. After the vulnerability is remediated, the R&D team of the relevant department is responsible for testing the vulnerability patch or version update. Huawei Cloud releases security notices (SNs) for discovered product or service vulnerabilities on its official website. You can view the SNs to learn about the impact scope, handling method, and threat level of the vulnerabilities. As for major vulnerabilities, the security O&M team maps out the scope of affected services and modules within minutes. There is also a security O&M team that necessary mitigation measures based on live network situations, for example, restricting port

access and implementing WAF rules on vulnerabilities to protect or isolate affected services, reducing the risk of vulnerability exploitation.

3.3.11 How does Huawei Cloud ensure that vulnerability remediation does not affect tenant services?

If a vulnerability needs to be addressed by installing a patch or a version update, gray release or blue-green deployment is used to minimize the impact on tenant services. On top of that, Huawei Cloud continuously updates the operating system and container images, and addresses system vulnerabilities through rolling upgrades of the images and containers, without affecting tenant services.

4 Infrastructure Security and Privacy Compliance

4.1 Data Center Security

4.1.1 Is Huawei Cloud infrastructure secure enough?

Infrastructure security is a core component of Huawei Cloud's multi-dimensional, full-stack cloud security system. We have enhanced the security and compliance of our data centers, networks, and other infrastructure based on industry best practices, so that you can migrate services to the cloud, stay focused on your business, and leave the security to us.

Our data centers are located in geographically secure locations. We take appropriate access control, monitoring, and service continuity assurance measures to improve the security and reliability of Huawei Cloud infrastructure. For details, visit the **Data Center** page at https://www.huaweicloud.com/intl/en-us/securecenter/security/datacenter.

We divide and isolate security zones and network planes in compliance with ITU-T E.408 standards and industry best practices.

For more information about the security design and practices of Huawei Cloud infrastructure, see *Huawei Cloud Security White Paper*.

4.1.2 How is the O&M security of data centers ensured?

All infrastructure in Huawei Cloud data centers uses a 2N backup system for rapid capacity expansion, and the capacity in Huawei Cloud data centers is planned to meet service requirements for the next five years or more. Huawei Cloud monitors access control, fire extinguishing systems, environment control, and physical security to ensure data center security.

Devices in the data center are properly installed and protected with highly visible and difficult-to-remove labels. The environment parameters of the data center are monitored in real time. When an exception is detected, an alarm is generated in real time and the responsible team is notified.

4.1.3 How does Huawei Cloud protect assets, such as computers, systems, and software?

Only software specifically allowed by Huawei can be installed on the office computers of Huawei Cloud. Non-standard software required for business must be scanned by Huawei

antivirus software before being installed. In addition, installing or using any pirated or cracked software on office computers is strictly prohibited.

Huawei Cloud deploys antivirus software to provide antivirus functions and firewalls in Windows. It uses the host-based intrusion detection system (HIDS) to protect ECSs and reduce the risk of account theft by providing functions such as weak password detection, malicious program detection, two-factor authentication, vulnerability management, and web page anti-tamper. In addition, the data loss prevention (DLP) software is installed on all Huawei Cloud terminals and is configured and managed by Huawei in a unified manner. Huawei Cloud configures software firewalls on terminals in a unified manner. The configurations cannot be modified by common users.

4.1.4 What are the physical and environmental cyber security requirements? If a data center is leased, how does Huawei Cloud ensure the implementation of these requirements?

Huawei Cloud has defined and implemented a complete set of physical and environmental security protection policies, procedures, and measures, meeting the Class-A requirements stipulated in GB 50174 Code for Design of Electronic Information System Room and T3 requirements stipulated in TIA-942 Telecommunications Infrastructure Standard for Data Centers.

If the data center is leased, Huawei Cloud raises requirements for suppliers based on the standards of Huawei's equipment rooms and specifies the requirements in the contracts with suppliers to ensure that suppliers provide services as required.

4.1.5 How do visitors or external personnel apply for permissions to enter or exit a data center? Where can the relevant records be found?

Huawei Cloud strictly manages the entry and exit of the data center. After obtaining approval, visitors accompanied by Huawei Cloud staff can access the low-level protection area, common controlled area, and other similar areas of the data center. They are not allowed to access the information system of the data center. They can access the specially-controlled area only after being approved by the data center administrator. Dedicated personnel are designated to review the visitor records of the data center every month.

Generally, Huawei Cloud does not directly disclose data center visitor records. If you want to access a Huawei Cloud data center, contact the customer manager.

4.1.6 How does Huawei Cloud maintain asset security?

Huawei Cloud classifies information assets based on ISO 27001 and uses dedicated tools to monitor and manage the assets. An asset list is generated, and each asset is assigned an owner.

4.1.7 How is the data processed when an asset is scrapped?

If a physical storage device is to be scrapped, Huawei Cloud deletes any data that was on it by means of degaussing, bending, or shredding the device as needed to ensure that the data stored on it cannot be restored.

4.2 Platform Security

4.2.1 How does the architecture of the cloud infrastructure provide security?

Huawei Cloud defines both security zones and service planes, and uses a network segregation strategy based on the security zoning principle of ITU E.408 and industry best practices for network security. Nodes in the same security zone are at the same security level. Huawei Cloud always takes a wide range of aspects of network security into full consideration, everything from how the network architecture is designed to device selection, configuration, and O&M. Huawei Cloud uses a set of network security systems to enforce stringent controls and ensure cloud security. Some key examples of these network security mechanisms are multi-layered security isolation, access control, and perimeter protection for physical and virtual networks. For details, see *Huawei Cloud Security White Paper*.

4.2.2 Is the production environment logically and physically isolated from the non-production environment?

Huawei Cloud keeps production and non-production environments both logically and physically isolated. Physical and logical network boundaries are used between the production environment and non-production environment. The duties of employees in the production environment and non-production environment are separated, and physical and logical access to the cloud environment is highly restricted.

4.2.3 How are the network security zones of the cloud infrastructure divided?

The Huawei Cloud data center network is divided into different security zones based on different business functions and security risks. The different zones are isolated using both physical and logical controls, which boosts the network immunity and fault tolerance in response to attacks from external actors and malicious insiders. The cloud infrastructure is divided into a DMZ, Public Services, Point of Delivery, Object-based Storage (OBS), and Operations Management (OM) zones. In addition to security zoning, distinct security levels within different security zones are also defined for Huawei Cloud. Attack surfaces and security risks are defined based on different business functions. For example, security zones that are directly exposed to the Internet have the highest security risks, but the OM zone, which does not include any interfaces exposed to the Internet, has a much smaller attack surface and lower security risks, and is less challenging to manage.

4.2.4 How does Huawei Cloud ensure that the management plane and tenant plane of the cloud platform are isolated and cannot access each other?

To ensure that services run by tenants do not affect Huawei Cloud administrative operations, different communication planes have been designed and built into Huawei Cloud's network based on their business functions, security risk levels, and access permissions. They include the tenant data plane, service control plane, platform O&M plane, and more. This ensures that network traffic for different purposes is reasonably and securely kept in separate lanes, which helps ensure separation of duties, roles, and responsibilities. In addition, Huawei Unified Virtualization Platform (UVP) uses security isolation for CPU, memory, and I/O resources. For details, see *Huawei Cloud Security White Paper*.

4.2.5 How does Huawei Cloud ensure that resources, networks, and data of different tenants are effectively isolated?

Huawei Cloud uses multi-layer security controls to implement resource isolation between tenants. Huawei UVP uses technologies such as CPU isolation, memory isolation, and I/O isolation to isolate tenant VM resources, so that one tenant cannot access other tenants' resources. In addition, a hypervisor is used to logically isolate the VMs of the same host on the network layer, and traditional physical network devices (such as routers and switches) are used for physical isolation between hosts. Huawei Cloud facilitates data isolation on the cloud through the Virtual Private Cloud (VPC) service. The VPC uses the network isolation technology to isolate tenants at Layer 3. For details, see *Huawei Cloud Security White Paper*.

4.2.6 How is tenant data cleared when tenant resources expire or a tenant is deregistered?

Huawei Cloud uses physical or digital methods to permanently destroy data. When a customer proactively deletes data stored on the cloud or the data needs to be deleted due to service expiration, Huawei Cloud will delete the data in compliance with the data destruction standards and the agreement signed with the customer.

4.2.7 How does Huawei Cloud ensure the security and integrity of VM images during lifecycle management?

Huawei Cloud encrypts public VM images and stores them in secure locations. In addition, it implements multiple security controls, such as access control, to ensure the availability, confidentiality, and integrity of the images. Huawei Cloud's professional security team performs system hardening on public images and patches any system vulnerabilities that may occur. Secure public images are created with the help of an image factory and provided to users through the Image Management Service (IMS). The IMS comes with secure cryptographic algorithms and functions. When a VM is created from an image, the integrity of the image is verified automatically to ensure that it is complete. Pertinent hardening and patch information is also provided to tenants for reference during image testing, troubleshooting, and other O&M activities.

4.2.8 Is system hardening performed for the operating system?

Huawei Cloud generates the security baseline for the operating system based on industry standards and actual situations. The operating system is configured according to the security baseline, and provides only the ports, protocols, and services necessary to meet service requirements. In addition, to ensure baseline security, Huawei Cloud addresses vulnerabilities and other issues (including baseline updates) of the operating system based on an established security patch management process.

4.2.9 Are anti-malware programs that support or connect to cloud service products deployed on all Huawei Cloud systems?

Huawei Cloud has deployed an IPS, WAF, antivirus software, and HIDS to manage the vulnerabilities of system components and networks. The IPS detects and prevents potential network intrusions. The WAF is deployed at the network border to protect application software. The antivirus software provides virus protection and firewalls in the Windows operating system. The HIDS protects ECSs and reduces the risk of account theft by providing functions

such as weak password detection, malicious program detection, two-factor authentication, vulnerability management, and web page anti-tamper.

Huawei Cloud provides tenants with services such as the Host Security Service (HSS), WAF, Managed Threat Detection (MTD), and Cloud Firewall (CFW) to detect, prevent, and recover from malware attacks.

4.2.10 Are secure and encrypted communication channels used to migrate physical servers, applications, or data to virtual servers?

Huawei Cloud uses VPNs to establish a secure encrypted communication channel that complies with industry standards between a remote network and a tenant VPC. A tenant's existing traditional data center is seamlessly connected to Huawei Cloud while ensuring end-to-end data confidentiality. Currently, Huawei Cloud uses an IPsec VPN together with IKE to encrypt data transport and ensure transport security. Huawei Cloud supports data transmission in REST and Highway modes, both supporting TLS 1.2 for encrypting data in transit.

Huawei Cloud provides multiple services to help you securely migrate data, such as the Server Migration Service (SMS) and Cloud Data Migration (CDM). In addition, the KooGallery provides a variety of migration services.

4.2.11 How are attacks on webs, APIs, and applications detected and intercepted?

Coupled with multi-layered advanced boundary protection, including anti-DDoS, IPS, and WAF, the API Gateway can effectively protect against numerous threats and attacks. By offloading the decryption of TLS encrypted traffic to the load balancer, the multi-layered advanced boundary protection is able to monitor plaintext traffic over the API Gateway and block attacks as needed. The API Gateway is a unique security perimeter for cloud services. It is built on an advanced perimeter protection system and provides protection measures such as ACL rule-based access restriction and replay attack prevention. For details, see *Huawei Cloud Security White Paper*.

4.2.12 How does Huawei Cloud ensure the high availability of infrastructure?

Using industry best practices, Huawei Cloud has deployed multiple data centers around the world for mutual backup. If one data center fails, the system automatically transfers customer applications and data out of the affected area to guarantee service continuity while ensuring compliance.

In addition to providing high-availability infrastructure, data redundancy and backup, and disaster recovery between AZs, Huawei Cloud also provides a service continuity plan, which it uses for regular testing. This plan aims to ensure service continuity even in the event of a major disaster, such as an earthquake or public health crisis. The service continuity plan helps you protect your services and your data.

4.2.13 Where can I obtain the service continuity certificates of the Huawei Cloud platform?

You can download related certificates in the **Download Compliance Certificates** section from the Compliance Center.

Compliance Center: https://www.huaweicloud.com/intl/en-us/securecenter/compliance

4.2.14 What services or capabilities does the Huawei Cloud platform provide to ensure tenant account security?

Huawei Cloud deploys the IAM service to ensure tenant account security. For details, see the IAM product overview page of Huawei Cloud.

IAM: https://www.huaweicloud.com/intl/en-us/product/iam

4.2.15 Does Huawei Cloud provide data encryption services for tenants?

Huawei Cloud provides the DEW service. It is a comprehensive cloud data encryption service that delivers functions such as dedicated encryption, key management, and key pair management. It uses Hardware Security Modules (HSMs) to protect the security of keys. It can be integrated with other Huawei Cloud services. For details, see the DEW overview page of Huawei Cloud.

DEW: https://www.huaweicloud.com/intl/en-us/product/dew

4.2.16 How does the Huawei Cloud platform allocate keys to tenants through the Key Management Service (KMS)?

When encrypting data on Huawei Cloud services, you need to specify a Customer Master Key (CMK). Then Huawei Cloud services generate a plaintext Data Encryption Key (DEK) and a ciphertext DEK. The ciphertext DEK is generated by encrypting the plaintext DEK using the specified CMK. Huawei Cloud services use the plaintext DEK to encrypt data. Encrypted data and the ciphertext DEK are stored together in Huawei Cloud services.

4.2.17 What audit functions required by tenants does Huawei Cloud provide?

Huawei Cloud has services such as the Log Tank Service (LTS), Cloud Eye Service (CES), and Cloud Trace Service (CTS), which make it possible for you to perform audits on demand.

4.2.18 How are security incidents handled?

Huawei Cloud has a mature security incident handling process. In this process, incidents are handled immediately upon detection. If you are directly affected by a security incident, Huawei Cloud will assign dedicated personnel to notify you, discuss a solution, and minimize the impact.

4.2.19 Are security incident response plans regularly tested?

Huawei Cloud tests the security incident response plan on an annual basis.

4.2.20 What should we do to secure our services on the cloud?

Huawei Cloud is committed to ensuring the security of the IaaS, PaaS, and SaaS cloud services and infrastructure on Huawei Cloud. You are expected to configure and use cloud services appropriately based on service requirements, so you can establish a comprehensive cloud security system.

In addition, you need to take security measures during each phase of a cloud migration.

4.2.21 What services can we use to improve cloud security?

Backed by years of experience with data security, Huawei Cloud provides a series of multi-dimensional and in-depth security services that integrate hardware and software.

On the **Security & Compliance** page of Huawei Cloud, you can find services to manage the security posture of your systems, such as Situation Awareness (SA) and MTD. You can also find the HSS and CFW, which can protect cloud workloads and applications. There are also many data security services that can protect your data assets on the cloud, including the Data Security Center (DSC) and DEW. You can easily build a comprehensive security system based on Huawei Cloud infrastructure and security services.

Security & Compliance: https://www.huaweicloud.com/intl/en-us/product/

4.2.22 What do customers need to do to meet security and compliance requirements?

Security and compliance responsibilities are shared between Huawei Cloud and our customers. Huawei Cloud is responsible for the security compliance of the cloud services, and the customers are responsible for the security and compliance of the services inside their organizations.

Huawei Cloud is always making changes to keep up with changing internal and external compliance requirements and to ensure the legal and regulatory compliance of cloud services. We strictly enforce security standard evaluations in a range of industries and share compliance practices with tenants to keep services transparent.

You need to check the applications and services that you deploy on Huawei Cloud but do not belong to Huawei Cloud against the applicable security laws and regulations.

For more information about Huawei Cloud certifications, as well as legal and regulatory compliance, check the Compliance Center and Resource Center.

- Compliance Center: https://www.huaweicloud.com/intl/en-us/securecenter/compliance
- Resource Center: https://www.huaweicloud.com/intl/en-us/securecenter/resource

5 Change History

Date	Version	Description
August 2024	1.2	Routine update
June 2024	1.1	Routine update
May 2023	1.0	First release