FAQS ABOUT PUBLIC CLOUD SERVICES FOR SINGAPORE GOVERNMENT AGENCIES

⊂−⊃ Alibaba Cloud

alibabacloud.com

⊂−⊃ Alibaba Cloud

LEGAL NOTICES

Alibaba Cloud **reminds you to carefully read through and completely understand all content in this section before you read or use this document. If you read or use this document, it is considered that you have identified and accepted all contents declared in this section.**

1. You shall download this document from the official website of *Alibaba Cloud* or other channels authorized by *Alibaba Cloud*. This document is only intended for legal and compliant business activities. The contents in this document are confidential, so you shall have the liability of confidentiality. You shall not use or disclose all or part of contents in this document to any third party without written permission from *Alibaba Cloud*.

2. Any sector, company, or individual shall not extract, translate, reproduce, spread, or publicize, in any method or any channel, all or part of the contents in this document without written permission from *Alibaba Cloud*.

3. This document may be subject to change without notice due to product upgrades, adjustment, and other reasons. *Alibaba Cloud* reserves the right to modify the contents in this document without notice and to publish the document in an authorized channel from time to time. You shall focus on the version changes of this document, download and get the updated version from channels authorized by *Alibaba Cloud*.

4. This document is only intended for product and service reference. *Alibaba Cloud* provides this document for current products and services with current functions, which may be subject to change. *Alibaba Cloud* makes the best efforts to provide an appropriate introduction and operation guide on the basis of current technology, but *Alibaba Cloud* does not explicitly or implicitly guarantee the accuracy, completeness, suitability, and reliability of this document. *Alibaba Cloud* does not take any legal liability for any error or loss caused by downloading, using, or putting trust in this document by any sectors, company, or individuals. In any case, *Alibaba Cloud* does not take any legal liability for any indirect, consequential, punitive, occasional, incidental, or penalized damage, including profit loss due to use of or trust to this document (even if *Alibaba Cloud* has notified you it is possible to cause this kind of damage).

5. All content, including, but not limited to images, architecture design, page layout, description text, and its intellectual property (including but not limited to trademarks, patents, copyrights, and business secrets) in this document are owned by *Alibaba Cloud* and/or its affiliates. You shall not use, modify, copy, publicize, change, spread, release, or publish the content from the official website, products, or programs of *Alibaba Cloud* without the written permission from *Alibaba Cloud* and/or its affiliates. Nobody shall use, publicize, or reproduce the name of *Alibaba Cloud* for any marketing, advertisement, promotion, or other purpose (including, but not limited to, a separate or combined form to use the name, brand, logo, pattern, title, product or service name, domain name, illustrated label, symbol, sign, or similar description that may mislead readers and let them identify it comes from *Alibaba Cloud* and/or its affiliates, of or from *Alibaba Cloud*, Aliyun, Wanwang, and/or its affiliates) without the written permission from *Alibaba Cloud*.

6. If you find any error or mistake in this document, directly contact *Alibaba Cloud*.

FAQS

1. Are Government Agencies Allowed to Use Alibaba Cloud?

As per requirement in Policy for Systems Using Commercial Cloud, agencies shall subscribe to the Government on Commercial Cloud System (GCCS) for cloud hosting services with **Official-Closed** and **Restricted** data. As such, agencies shall determine the final classification tier of the system before subscribing to cloud services. Where applicable, Agencies shall implement the security safeguards to protect sensitive data.

Agencies can subscribe to Alibaba Cloud services for Official-Open systems with Non-Sensitive data used by agency offices. Alibaba Cloud provides solutions of tokenization to prevent moving your sensitive data to public cloud computing environment.
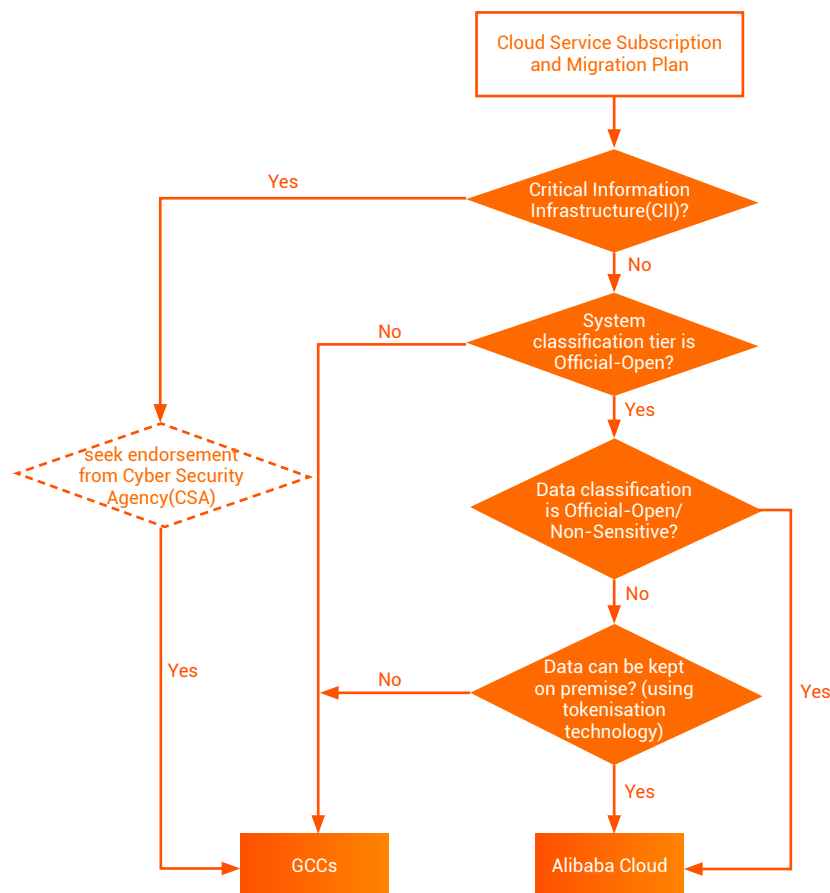
FAQS

2. What are the Relevant Government Policies When Agencies Using Public Cloud Services?

Agencies are required to comply with the estipulate clauses in policy for systems using commercial cloud and the list of clauses indicated in ANNEX C - Applicable IM8 clauses for commercial cloud. Alibaba Cloud is able to comply with the applicable requirements or provides security features to help agencies in complying the relevant requirements.

3. How does Alibaba Cloud Comply with Government Policies?

Alibaba Cloud looks at Policy for Systems Using Commercial Cloud, and complies with the applicable requirements. Meanwhile, Alibaba Cloud provides security measures enabling agencies in complying with the requirements. Please refer to below responses that are relevant to Policy for Systems Using Commercial Cloud.

Auditing of Cloud Services

Alibaba Cloud is certified under CSA STAR, and other internationally recognized security standards, such as ISO27001, ISO27107, ISO27018, ISO27701, and ISO22301. Meanwhile, Alibaba Cloud provides SOC 1 & 2 type II report, which provides a description of Alibaba Cloud's internal controls with an opinion from the independent auditor to assure that the controls have been designed and operated effectively to achieve the AICPA Trust Services Criteria relevant to security, availability, and confidentiality. Alibaba Cloud's security certificates, CSA CCM and SOC reports are available for downloading via Trust Center. https://www.alibabacloud.com/trust-center [M2.6]

FAQS

Security Monitoring and Incident Management

Alibaba Cloud's Security Center is a unified security management system that identifies, analyzes, and produces alerts based on security threats in real time, providing central visibility and security incident monitoring of Cloud assets. Agencies can rely on the capabilities offered by Security Center in monitoring security related events. Besides, Alibaba Cloud's Object Storage Service (OSS) helps the agencies to retain the logs generated for at least one year. [M2.7 & 2.9]

Security Measures for Cloud services

a. Security Configuration

Alibaba Cloud has security hardening standards in place. Alibaba Cloud offers Aliyun Linux 2, a next-generation Linux distribution released by Alibaba Cloud. Agencies can follow the security best practices (i.e. remediations) in the CIS Benchmark to enhance OS security, or use the CIS Benchmark Remediation Kit to automatically harden Aliyun Linux 2. [M2.12a]

b. Log Management

Alibaba Cloud's Log Service stores logs in a distributed file system, and uses a triplicate distributed storage mechanism to ensure data reliability and durability. Log Services also provides capabilities to store log archives to OSS bucket. [M2.12c]

FAQS

c. Network Security

Alibaba Cloud's Virtual Private Cloud (VPC) can help build an isolated virtual network environment. The intranet communication within a VPC is completely isolated from other users and other VPCs even under the same account. In addition, Alibaba Cloud Firewall is the industry's first firewall as a service (FWaaS) solution targeted for public clouds. It centrally manages control policies for the access traffic from the Internet to Elastic Compute Service (ECS) instances (Internet traffic), and provides micro-isolation policies for the access traffic between ECS instances (intranet traffic). [M2.12e]

d. Intrusion Prevention

Alibaba Cloud Firewall integrates Intrusion Prevention Service (IPS) and threat intelligence capabilities for intrusion detection and analysis. By default, Cloud Firewall can also store network traffic and security event logs and firewall operation logs for six months. [M2.12f]

e. Remote Administration Management

Alibaba Cloud Bastionhost enables remote administration to systems or applications remotely. It provides capabilities to manage asset O&M permissions in a centralized manner, monitor all O&M operations, and reproduce O&M scenarios in real time to facilitate identity authentication, access control, and operation audit. [M2.12g]

FAQS

f. Vulnerability Management

Alibaba Cloud Security Center provides capabilities to scan for vulnerabilities and security threats based on installed the lightweight Security Center agent on VMs. Security Center can help agencies scan and fix multiple systems and applications simultaneously during O&M. Currently, Security Center can detect mainstream vulnerabilities in Windows, Linux, and Web-CMS systems and applications. It can also offer vulnerability detection and patching capabilities in applications for which official patches are unavailable. [M2.12h]

Alibaba Cloud market place provides vulnerabilities scanning and penetration testing services which are provided by our eco-system partners. In addition, Alibaba Cloud provides a Managed Security Service, where a team of security experts will perform vulnerability assessment and security test. [M2.12i]

g. Virus Detection

Security Center can also intercept mainstream viruses such as ransomware, mining scripts, and DDoS trojans in real time. It monitors and analyzes files and processes at the virtual machine's system kernel level in real time, and can effectively overcome the anti-detection technologies of trojans and malware. [M2.12j]

FAQS

Data Recoverability

Alibaba Cloud offers Hybrid Backup Recovery (HBR) service, which allows agencies to back up data stored in ECS instances, Apsara File Storage NAS, OSS, on-premises data centers, and VMware virtual machines. HBR also support migrating data from VMware virtual machines to Alibaba Cloud. In addition, agencies can restore the data from a backup file from HBR. [M2.17]

Data Security

Alibaba Cloud is able to provide security measures or capabilities to protect agencies data in accordance with the requirements in M2.20.

a. Alibaba Cloud allows agencies to encrypt data stored at rest in Alibaba Cloud services with integration of Alibaba Cloud Key Management Service (KMS). Alibaba Cloud services including EBS, OSS, RDS, Table Store, NAS, MaxCompute, support Data encryption at rest. When an agency uses the data encryption feature of an Alibaba Cloud service for the first time, the system automatically creates a Customer Master Key (CMK) exclusively for the service in the user's KMS for the specific region in which the service is being used. Subsequently, the agency can manage the lifecycle of CMK by KMS.

b. Cloud products use the SSL/TLS protocol to ensure data transmission security while users read and upload data. By setting a TLS security policy (with supported TLS protocol versions and cipher suites) in a SLB instance, agencies can establish a security protocol for data transmission from public networks to Alibaba Cloud VPCs.

Alibaba Cloud Certificates Service can issue SSL certificates issued by well-known third-party certification authorities on the cloud to enable HTTPS for websites so that the websites are protected against traffic hijacking, tampering, and interception.

FAQS

c. The Alibaba Cloud console uses HTTPS encryption for data transmission. Alibaba Cloud products provide API access points that have HTTPS encryption enabled with 256-bit key length to address the need for encrypted transmission of sensitive data. For remote administration, Alibaba Cloud VPN Gateway can be used to provide secure connections, particularly connections between a non-premises data center, office networks, Internet terminals, or Alibaba Cloud VPC through encrypted channels.

d. Alibaba Cloud KMS offers managed HSM services, based on FIPS 140-2 Level 3 validated HSMs, providing high security assurance for cryptographic keys, enabling agencies to protect their most sensitive workloads and assets, and to meet regulatory compliance. In addition, Alibaba Cloud Data Encryption Service, allows agencies to generate and use the encryption keys on HSM that is FIPS 140-2 Level 3 validated. It also allows agencies to access tamper-resistant HSM instances in their Alibaba Cloud VPC in an exclusive and single-tenant manner to protect the encrypted keys.

e. KMS is integrated with ActionTrail. Agencies can use ActionTrail to query the records of all events that are triggered by all users on KMS resources. The agencies can also store the KMS usage information in other services such as OSS to meet audit requirements in the long term.

f. As a fully managed distributed service, KMS builds multi-zone redundant cryptographic computing capabilities in each region to ensure reliability and availability. KMS ensures key security by containing keys within certain security boundaries and forbidding cross-boundary key distribution, and provides a cryptographic function through a specific interface for cryptographic operations.

g. On terminating an agency's services, Alibaba Cloud deletes the agency's data assets in a timely manner or returns the data assets according to relevant agreements. Alibaba Cloud uses data erasure techniques that meet industry standards. The erasure operations are logged to prevent unauthorized access to agency's data.