# 华为云巴西政府云计算安全遵从性指南

**文档版本** 1.0

**发布日期** 2022-09-12

**华为云计算技术有限公司**

### 商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

### 注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

## 华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

# 目 录

# 1 概述

## 1.1 背景和发布目的

随着技术的发展，对云计算的使用已经成为巴西联邦政府机构的常态。云计算为联邦政府机构的信息化发展带来巨大的好处，但它也为联邦政府机构创造了一个复杂的环境。为规范政府行业对于云计算解决方案的运用，巴西共和国总统/机构安全办公室发布了No.5规范指令（NORMATIVE INSTRUCTION NO. 5），指令规定了联邦政府机构和实体使用云计算解决方案的最低信息安全要求。

华为云作为云服务供应商，致力于协助联邦政府机构客户满足这些监管要求，持续为政府行业客户提供遵从政府行业标准要求的云服务及业务运行环境。本文将针对巴西联邦政府机构或实体在使用云服务时通常需遵循的信息安全监管要求和指南，详细阐述华为云将如何协助其满足信息安全监管要求。

## 1.2 关于联邦政府云计算最低信息安全要求的《NO.5 规范性指令》简介

- **NO. 5规范指令**

巴西共和国总统/机构安全办公室于2021年8月30号（自发布日期起生效），发布了**No.5规范指令（NORMATIVE INSTRUCTION NO. 5）**，指令规定了联邦政府机构和实体使用云计算解决方案的最低信息安全要求。

作为已经使用或者希望使用云计算的联邦政府机构或实体应遵守的最低信息安全要求的指南，一方面，指令要求联邦政府机构或者实体需建立云计算安全管理组织与制度，另一方面，指令规定了联邦政府机构或实体在使用云计算服务提供商提供的服务时，需要满足的最低的信息安全管理或技术要求。

## 1.3 名词定义

- **华为云**

华为云是华为的云服务品牌，致力于提供稳定可靠、安全可信、可持续创新的云服务。

- **云计算**

根据美国国家标准技术研究院（ NIST ）的定义，是指一种基于互联网，能够按需提供共享计算机处理资源和数据的计算模式。

- **客户**

与华为云达成商业关系的注册用户。

- **云代理（Ocloud broker）**

云代理应充当联邦政府机构或实体与两个或多个云服务提供商之间的云计算服务的集成商。

# 2 华为云认证情况

华为云继承了华为公司完备的管理体系以及IT系统的建设和运营经验，对华为云各项服务的集成、运营及维护进行主动管理，并持续改进。截至目前，华为云已获得众多国际和行业安全合规资质认证，全力保障客户部署业务的安全，主要包括：

**全球性标准类认证**

| 认证 | 产品介绍 |
| --- | --- |
| ISO 20000:2011 | ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的IT服务来满足客户和业务的需求。 |
| ISO 27001:2013 | ISO 27001是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。 |
| ISO 27017:2015 | ISO 27017是针对云计算信息安全的国际认证。ISO 27017的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。 |
| ISO 22301:2012 | ISO 22301是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。 |
| SOC审计 (SOC 1 Type II, SOC 2 Type II, SOC 3) | SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况 出具的独立审计报告。华为云已获得SOC 1 Type II, SOC 2 Type II和SOC 3鉴证审计报告三项权威认证，其中SOC 2 五大控制属性审计全部通过，为全球首家，表明华为云平台的信息安全管理能力已达到国际公认的最高标准，能够为您提供世界一流的安全隐私保障及服务。 |
| PCI DSS认证 | 支付卡行业数据安全标准（PCI DSS）是由JCB、美国运通、Discovers万事达和Visa等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。 |

| | |
|---|---|
| CSA STAR 金牌认证 | CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安 全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨 在应对与云安全相关的特定问题，协助云计算服务商展现其服务成 熟度的解决方案。 |

| 认证 | 产品介绍 |
|---|---|
| 国际通用准则 CC EAL3+ | CC（Common Criteria）认证是一种信息技术产品和系统安全性的评估 标准，它提供了一组通用的安全功能要求和安全保证要求，并在这 些保证要求的基础上提供衡量IT安全性的尺度（即评估保证级EAL），使得独立的安全评估结果可以互相比较。 |
| ISO 27018:2014 | ISO 27018是专注于云中个人数据保护的国际行为准则。ISO27018的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。 |
| ISO 29151:2017 | ISO 29151是国际个人身份信息保护实践指南。ISO 29151的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。 |
| ISO 27701:2019 | ISO 27701规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过IS O27701表明了其在个人数据保护具有健全的体制。 |
| BS 10012:2017 | BS 10012是BSI发布的个人信息数据管理体系标准，BS10012认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。 |
| PCI 3DS | PCI 3DS标准旨在保护执行特定3DS功能或者存储3DS数据的3DS环境，支持3DS的实施。PCI 3DS认证的通过表明华为云在3D协议执行环境的过程、流程、人员管理等方面符合安全标准。 |

**地区性标准类认证**

| 认证 | 产品介绍 |
|---|---|
| OSPAR认证（新加坡） | TISAX（ Trusted Information Security Assessment Exchange，可信 信息安全评估交换）是德国汽车工业联合会（VDA ）联合欧洲汽车 工业安全数据交换协会（ENX ）推出的汽车行业信息安全评估和数据 交换安全标准。TISAX认证的通过，表明华为云已满足欧洲认可的汽 车行业信息安全标准。 |
| MTCS Level 3认证（新加坡） | MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level 3等级认证。 |
| OSPAR认证（新加坡） | OSPAR是新加坡银行业工会（ABS ）对外包服务提供商出具的审计报 告。华为云通过了新加坡银行协会（ABS）关于控制外包服务提供商的 目标和流程的指南（ABS指南），证明了华为云是符合ABS指南中规 定的控制措施的外包服务提供商。 |

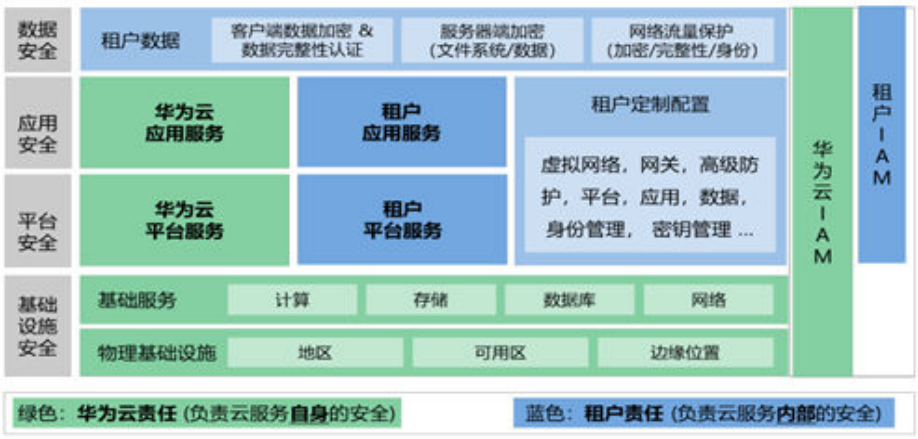
| | |
|---|---|
| 网络安全等级保护（中国） | 网络安全等级保护是中国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键Region、节点通过了网络安全等级保护四级。 |
| 可信云金牌运维专项评估（中国） | 金牌运维评估是面向已通过可信云服务认证的云服务供应商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、健全的运维管理体系，符合国内权威云服务运营和维护保障要求的认证标准。 |
| 云服务用户数据保护能力认证（中国） | 云服务用户数据保护能力评估是针对云服务用户数据安全的评估机制，评测关键指标范围包括事前防范、事中保护、事后追溯三个层面。 |
| 工信部云计算服务能力评估（中国） | 云计算服务能力评估是以《信息技术云计算云服务运营通用要求》等相关国家标准为依据的分级评估标准。华为私有云和公有云双双获得云计算服务能力“一级”符合性证书。 |
| 可信云评估（中国） | 可信云评估是由数据中心联盟（DCA）组织、中国信息通信研究院（工信部电信研究院）测评的面向云计算服务和产品的权威评估。 |
| 网信办网络安全审查（中国） | 网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。 |

关于更多华为云的安全合规信息以及获取相关合规证书，可参见华为云官网"**信任中心-合规中心**”。

# 3 华为云安全责任共担

在复杂的云服务业务模式中，云安全不再是某一方单一的责任，需要租户与华为云共同努力。基于此，华为云为帮助租户理解双方的安全责任边界、避免出现安全责任真空区而提出了责任共担模型。在模型中租户与华为云具体负责的区域可参见下图。

**图 3-1** 华为云安全责任共担模型




基于责任共担模型，华为云与租户主要承担如下责任：

**华为云：**主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和租户身份管（IAM）层的多维立体安全防护体系，并保障其运维运营安全。

**租户：**主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和IAM层的各项安全防护措施的定制配置、运维运营安全、以及用户身份的有效管理。

关于华为云与租户的安全责任详情，可参考华为云已发布的**《华为云安全白皮书》**。

# 4 华为云全球基础设施

华为云目前已陆续在全球多个国家或地区开服。华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云客户能够根据实际需求决定在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，此外，华为严格遵守当地规定，不接触客户数据。每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。关于更多关于华为云基础设施的信息，参见华为云官网“**全球基础设施**”。

# 5 华为云如何遵从及协助客户满足《 NO. 5 规范指令 》要求

巴西《 No.5规范指令 》规定了联邦政府机构或者实体使用云计算解决方案的最低信息安全要求。联邦政府机构在遵循《 No.5规范指令 》要求时，华为云作为云服务提供商，可能会参与到要求所涉及的活动中，以下内容将总结该规范指令中与云服务提供商相关的控制要求，并阐述华为云作为云服务提供商，如何协助联邦政府机构或实体客户满足这些控制要求。

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| Art.13 | 安全采用云计算的要求：身份和日志管理 | 在身份和记录的管理方面，各政府机构或实体至少应：<br>I -采用联合身份标准，允许在云服务提供商的用户身份验证过程中使用单点登录技术；<br>II -拒绝许可云服务提供商使用和直接访问政府机构或实体的身份验证环境的权限；<br>III根据信息的临界程度，采用单点登录技术，该技术中必须伴之以：<br>（a）多因素身份验证；或<br>（b）采用另一种选择，即，提高云服务提供商中，其用户身份验证过程中的安全性；<br>IV -要求云服务提供商：<br>（a）记录所有网络访问，事件记录，包括有关会话和交易的信息；和<br>（b）将（a）点所述的所有记录保存一年；<br>V -由签约政府机构或实体自行决定，在云服务提供商的环境或其自己的受控环境中，将所有网络访问和事件的记录（包括有关会话和交易的信息）保存五年；<br>VI -在自己的受控环境中将所有网络访问和事件的记录（包括从云服务提供商收到的有关会话和交易的信息），保存五年；和<br>VII -授权安全团队访问和使用云服务提供商生成的记录。 | 客户应采用联合身份标准、多因素认证方式和单点登录技术，客户必须在受控环境中存储所有网络访问和事件记录5年。由他们决定是否将其存储在云中。华为云作为云服务提供商，为配合客户满足身份管理的要求：<br>1. 提供**统一身份认证服务（Identity and Access Management，简称IAM）**，对使用云资源的用户账号进行管理。<br>1. IAM提供适合企业级组织结构的用户账号管理服务，为企业用户分配不同的资源及操作权限。用户通过使用访问密钥获得基于IAM的认证和鉴权后，以调用 API 的方式访问华为云资源。<br>2. 如果租户有安全可靠的外部身份认证服务商，可以将IAM服务的联邦认证外部用户映射成华为云的临时用户，并访问租户的华为云资源。<br>3. IAM 可以按层次和细粒度授权，保证同一企业租户的不同用户在使用云资源上得到有效管控，避免单个用户误操作等原因导致整个云服务的不可用，确保租户业务的持续性。<br>1. 华为云支持单点登录技术进行身份验证，在一个多系统共存的环境下，用户的一次登录能得到其他所有系统的信任。<br>2. 多因子认证：是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信认证码进行二次认证。用户修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 3. 华为云作为云服务提供商，内部制定了日志管理规范，保存所有的平台侧网络网络记录1年，包括有关会话和交易的信息。同时，指令要求机构在受控环境中存储所有的网络访问和事件记录5年，可自行决定是否存储在云环境中。为配合客户满足日志管理监管要求，华为云提供**云日志服务（Log Tank Service，简称LTS）**提供日志收集、实时查询、转储等功能，可长期保存日志。主机和云服务的日志数据上报至LTS后，存储时间可以在1-30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）、数据接入服务（DIS）中长期保存。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| Art.14 | 安全采用云计算的要求：加密资源 | 关于使用加密资源的需要，政府机构或实体至少应：<br>I -验证组织的数据是否被依法进行处理和存储；<br>II -根据法律要求、风险、关键程度、成本和收益分析数据加密的必要性；和<br>III -尽可能使用基于硬件的加密密钥。 | 客户应评估数据加密的必要性，并使用安全的加密技术对数据进行加密。<br>目前，华为云**云硬盘（ Elastic Volume Service，简称 EVS ）**、**对象存储服务（Object Storage Service，简称 OBS ）**、**镜像服务（Image Management Service-IMS ）**和关系型数据库等多个服务均提供数据加密（服务端加密）功能，采用高强度的算法对存储的数据进行加密。服务端加密功能集成了**数据加密服务（Data Encryption Workshop，简称 DEW ）的密钥管理功能，由DEW进行密钥全生命周期集中管理。**，DEW是一个综合的云上数据加密服务。它可以提供专属加密、密钥管理、密钥对管理等功能。其密钥由硬件安全模块（HSM）保护，并与许多华为云服务集成。用户也可以借此服务开发自己的加密应用。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，从而助力客户云上数据的安全。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| Art.15 | 安全采用云计算的要求：数据隔离和逻辑分离 | 关于云计算环境中的数据隔离和逻辑隔离，政府机构或实体应与云服务提供商一起，至少采取以下措施：<br>I -确保合同环境免受云环境服务的外部用户和未经授权的人员的侵害，并实施信息安全控制，以便为联邦公共行政部门的不同机关或实体以及云服务的其他用户使用的资源提供充分的隔离；<br>II -确保对虚拟化应用程序、操作系统、存储和网络数据进行适当的逻辑隔离，以便建立所用资源的分离；<br>III -确保云服务提供商使用的所有资源与该政府机构或实体内部管理使用的资源分开；和<br>IV -评估安装在云服务中运行的专有软件相关的风险。 | 客户在使用云服务之前，应确认云服务提供有效的数据隔离和逻辑隔离。<br>华为云作为云服务提供商，提供逻辑隔，数据隔离，业务与管理、运维分离，帮助客户满足要求：<br>**逻辑隔离：**提供华为云平台操作系统——统一虚拟化平台（Unified Virtualization Platform，简称UVP）通过对服务器物理资源的抽象，将CPU、内存、I/O 等物理资源转化为一组统一管理、可灵活调度、可动态分配的逻辑资源，并基于这些逻辑资源，在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境。UVP直接运行于物理服务器之上，提供虚拟化能力，为虚拟机提供运行环境。UVP 通过 CPU 隔离、内存隔离和 I/O 隔离等技术手段实现虚拟主机操作系统与访客虚拟机操作系统之间的隔离，并通过 Hypervisor 让虚拟主机操作系统与访客虚拟机操作系统使用不同的权限运行，来保证平台系统资源的安全。<br>**数据隔离：**华为云对云端数据的隔离是通过虚拟私有云（VPC – Virtual PrivateCloud）实施的，VPC 采用网络隔离技术，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置：一方面，结合 VPN或云专线，将 VPC 与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用 VPC 的 ACL、安全组功能，按需配置安全与访问规则，满足租户更细粒度的网络隔离需要。<br>**业务与管理、运维分离：**为保证租户业务不影响管理操作，确保设备、资源和流量不会脱离有效监管，华为云将其网络的通信平面基于不同业务职能、不同安全 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 风险等级和不同权限需要划分为租户数据平面、业务控制平面、平台运维平面、BMC（Baseboard Management Controller）管理平面、数据存储平面等，以保证关乎不同业务的网络通信流量得到合理且安全的分流，便于实现职责分离。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| Art.16 | 安全采用云计算的要求：云管理 | 在云管理方面，政府机构或实体至少应做到：<br>I -授权负责云管理的团队使用云服务提供商所使用的技术；<br>II -要求云服务提供商记录和传达其信息安全资源，角色和使用其云服务的责任；<br>III-明确各方责任，包括云管理团队本身的义务和责任；和<br>IV -与云服务提供商一起制定事件处理流程，并将其传达给负责云管理的团队。 | 客户应制定事件处理流程。<br>在责任共担模型中，明确华为云与华为云租户承担的责任，华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 各类各项云服务自身的安全，华为云租户承担云内安全与配置责任。<br>作为云服务提供商，华为云内部依托其建立的漏洞管理体系进行漏洞管理，能确保基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在SLA时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响租户业务的风险。对于涉及云平台、租户服务等的漏洞，在确保不会因主动披露而导致更大攻击风险的情况下，向最终用户/租户及时推送漏洞规避和修复方案和建议，与租户共同面对安全漏洞带来的挑战。华为云还制定了不同产品的服务等级，为用户提供了高可用性的服务承诺。详情可参考**《华为云服务等级协议》**。<br>同时，华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。根据内部的客户通知通报流程，在底层基础平台发生严重事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| Art.18 | 安全采用云计算的要求：数据存储在巴西 | 机构或实体制作或维护的转移给云服务提供商的数据、元数据、信息和知识必须托管在巴西领土上，并遵守以下规定：<br>I - 必须在巴西领土上保存至少一份更新的备份副本；<br>II - 根据适用的立法，没有访问限制的信息可能在巴西领土以外更新了备份副本；<br>III-根据适用法律，法律规定的限制访问信息和第17条第Ⅱ项未规定的与预备文件及其更新的安全备份副本不能在巴西境外处理；<br>IV -就个人数据而言，必须遵守 2018年8月14日第13，709号法律，个人数据保护一般法 -LGPD以及有关该主题的其他立法中规定的准则。 | 客户应确保：受限的数据只能在巴西领土范围内处理；转移给云服务提供商的数据必须在巴西领土上至少保留一份最新的数据备份。<br>华为云在圣保罗建立了数据中心，客户选择在巴西境内实现上云（详情参见“**全球基础设施**”），同时，华为云提供**云备份（Cloud Backup and Recovery，简称CBR）**，CBR为云内的云服务器、云硬盘、文件服务，VMware虚拟化环境，提供简单易用的备份服务，保障用户数据的安全性和正确性，确保业务安全。<br>华为云遵从巴西LGPD，详情参考**《华为云巴西 LGPD 遵从性说明》** |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| Art.19 | 安全采用云计算的要求：具体合同条款 | 与云服务提供商签署的提供云计算服务的合同文书应包含处理第10条至第18条中规定的要求，至少包括以下安全程序：<br>I - 保密条款，防止云服务提供商向国家，跨国，外国及外国政府使用、传输和发布来自政府机构或实体的数据，系统、流程和信息；<br>II - 保证机构或实体对合同期内处理的所有信息的专有权，包括任何可用的副本，例如安全备份；<br>III - 禁止云服务提供商使用来自政府机构或实体的信息用于广告宣传、优化人工智能机制或任何未经授权的二次使用；<br>IV - 使云服务提供商的信息安全政策符合巴西立法；<br>V - 在合同结束时将云服务提供商保管的数据、信息和系统完全返还给签约机构或实体；<br>VI - 云服务提供商在合同终止时，根据处理强制保留数据的法律，删除其托管的政府机构或实体的任何数据，信息或系统；和<br>VII - 根据2018年8月14日第13，709号法律第16条（LGPD），保障个人数据的被遗忘权。 | 在使用云服务时，客户应与云服务提供商签订具有法律效力合同文书，合同应包含保密条款、禁止云服务提供商使用客户数据等方面的内容。<br>1. 为配合客户满足监管要求，华为云提供了线上的**《华为云用户协议》**以及**《华为云服务等级协议》**，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。<br>2. 《华为云用户协议》中包含保密条款，规定各方保密义务，且华为云不会访问或者使用客户的内容，不会未经授权二次使用客户的数据。<br>3. 华为云信息安全政策：参照ISO27001构建了完善的信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性。全方位保护客户系统和数据的保密性、完整性和可用性。<br>4. 在合同结束时，客户可通过华为云提供的**对象存储迁移服务（Object Storage Migration Service，简称OMS）**和**主机迁移服务（Server Migration Service，简称SMS）**，将内容数据从华为云中迁移出去，如迁移至本地数据中心。<br>5. 当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格 |

| 原文编号 | 控制域 | 具体控制要求 | 华为云的应答 |
| --- | --- | --- | --- |
| | | | 遵循数据销毁标准以及与客户之间的协议约定，对客户数据进行清除。<br>6. 华为云遵从LGPD保障个人数据的被遗忘权，详情参考**《 华为云隐私保护白皮书 》** |

| | | | |
| --- | --- | --- | --- |
| Art.20 | 安全采用云计算的要求：对云服务提供商的要求 | 为了能够向政府机构或实体提供云计算服务，云服务提供商必须至少满足以下要求：<br>I - 根据最佳做法和立法制定风险管理方法，并进行第11条第 II 项所述的风险管理； | 在使用云服务时，客户应确定云服务供应商是否制定了网络风险管理机制，是否具备风险管理能力。<br>华为云继承了华为公司的风险管理能力，建立了完善的风险管理体系，对风险管理范围、风险管理组织以及风险管理过程中的标准进行了严格定义，并通过风险管理体系的持续运作，在复杂的内外部环境和巨大的不确定市场中有效控制风险，力求业绩增长和风险之间的最优平衡，持续管理内外部风险，保障公司持续健康发展。 |

| | | | |
|---|---|---|---|
| | | II - 实施加强虚拟化机制的做法，其中至少应包括以下程序：<br>（ a ）禁用或删除操作系统执行的所有不必要的接口、端口、设备或服务；<br>（ b ）安全地配置所有网络接口和虚拟存储区域；<br>（ c ）建立虚拟机资源使用限制（ 虚拟机 - VM）；<br>（ d ）保持虚拟机上所有操作系统和应用程序在其最新版本中运行；<br>（ e ）验证加密密钥管理操作的完整性；<br>（ f ）具有允许机构或实体的授权用户访问虚拟机监视器 -虚拟机管理程序的管理访问记录的控件；<br>（ g ）启用完整的 Hypervisor 日志记录；和<br>（ h ）支持使用由机构或实体提供的、符合云服务提供商要求的网络强化政策和实践的可信虚拟机（ trusted VM ）； | 在使用云服务时，客户应确认云服务提供商实施加强虚拟化机制的做法。<br>华为云作为云服务提供商，为客户提供**企业主机安全服务（ Host Security Service ，简称HSS ）**以帮助客户执行自动基线检查。或者客户通过**《 华为云安全基线配置指南 》**对云服务的安全基线进行检查和配置。华为云提供的加强虚拟化机制做法如下：<br>1. **端口管理：** 华为云可提供端口或接口管理的能力，禁用高危端口及远程管理端口，配置 VPC 实现网络隔离，配置 VPC 子网 ACL 规则、VPC 对等链接的安全配配置安全组入方向规则。<br>2. **VM使用限制：** 虚拟机可启用资源监控，监控虚拟机的资源使用情况，并进行监控告警。<br>3. **版本更新：** 华为云负责公共镜像的定期更新与维护，向用户提供安装安全补丁的公共镜像和相关安全加固和补丁信息，以便用户在部署测试、故障排除等运维活动时参考。<br>4. **加密密钥完整性验证**：当企业管理员使用运维工具或 API 命令管理华为云上的资源时，访问密钥用于对 API 请求进行签名，API 网关则校验签名信息。数字签名和时间戳可以防止数据传输过程中请求被篡改，确保消息完整性，并防止潜在的重放攻击。<br>5. **管理访问记录：** 华为云提供**云审计服务（ Cloud Trace Service，简称 CTS ）**为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的 API 执行的操作，以及华为云系统内部触 |

| | | | |
|---|---|---|---|
| | | | 发的操作。CTS 是满足用户专业认证以及 IT 合规性认证的不可或缺的支撑性服务。<br>6. **Hypervisor 日志记录：** Hypervisor一种运行在基础物理服务器和操作系统之间的软件层，可允许多个操作系统和应用共享硬件，也可成为虚拟机监视器。当服务器启动并执行Hypervisor时，它会加载所有虚拟机客户端的操作系统同时会分配给每一台虚拟机适量的内存，CPU，网络和磁盘。华为云已启用完整的Hypervisor日志记录，可以监控虚拟机使用情况，为云上运维提供信息支撑。<br>7. **可信虚拟机支持：** IMS提供了私有镜像的全生命周期管理能力，主要包括创建私有镜像，复制、共享或导出私有镜像等操作，客户可以根据实际场景选择合适的方法，并结合弹性云服务器、对象存储等周边服务完成业务上云或迁移。 |

| | | | |
|---|---|---|---|
| | | III - 关于身份和记录管理：<br>（ a ）具有访问控制程序，以解决角色之间的转换，限制和控制用户权限以及用户帐户的使用控制；<br>（ b ）实施身份验证机制，限制访问密码的长度、复杂性、持续时间和历史记录；<br>（ c ）支持单点登录技术进行身份验证；<br>（ d ）根据信息的关键程度，支持多因素身份验证机制或其他替代方案，以提高云服务提供商中机构或实体的用户身份验证过程中的安全性；<br>（ e ）允许机构或实体管理自己的身份，包括在云服务提供商提供的环境中创建、更新、删除和暂停；且<br>（ f ）满足政府机构或实体在其身份验证、访问控制、会计账户和注册过程（格式、保留和访问）中的法律、安全最佳实践和其他标准等要求； | 在使用云服务时，客户应确认云服务提供商建立访问控制管理机制，设定与职责匹配的用户权限，采用安全的身份认证和数据加密技术，并对用户访问通过日志进行记录。华为云提供的身份和记录管理能力如下：<br>华为云提供IAM对使用云资源的用户账号进行管理。IAM除了支持密码认证之外还支持多因素认证，客户可自主选择是否启用。<br>1. 提供IAM，支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。此外，IAM还支持客户的安全管理员设置登录策略，避免用户密码被暴力破解或者因为访问钓鱼页面等而导致账号信息泄露。<br>2. IAM 可以按层次和细粒度授权，保证同一企业租户的不同用户在使用云资源上得到有效管控，避免单个用户误操作等原因导致整个云服务的不可用，确保租户业务的持续性。<br>3. 华为云支持单点登录技术进行身份验证，在一个多系统共存的环境下，用户的一次登录能得到其他所有系统的信任。 |

| | | | |
|---|---|---|---|
| | | IV - 关于云环境中可用的Web应用程序的安全性：<br>（ a ）使用专门用于保护系统和应用程序的防火墙；<br>（ b ）根据安全开发最佳实践和现有法规开发网络代码；<br>（ c ）使用操作系统和应用程序安全的最佳做法；<br>（ d ）定期进行网络和应用程序渗透测试；和<br>（ e ）有漏洞纠正程序； | 在使用云服务时，客户应确认云服务提供商提供云环境中Web应用程序的安全保护能力，<br>1. 华为云提供 **Web 应用防火墙（ Web Application Firewalls，简称WAF ）**应对 Web 攻击，如 Web 应用层的 DDoS 攻击、SQL 注入、跨站脚本攻击（ Cross-Site Scripting，简称 XSS ）、跨站请求伪造（ Cross-Site Request Forgery，简称 CSRF ）、组件漏洞攻击、身份伪造等，以保护部署在 DMZ 区、面向外网的 Web 应用服务和系统。<br>2. 华为云严格遵从华为对内发布的安全编码规范。华为云服务研发和测试人员在上岗前均通过了对应规范的学习和考试。同时引入了静态代码扫描工具每日检查，其结果数据进入云服务持续集成和持续部署（ Continuous Integration， Continuous Deployment，简称 CI/CD ）工具链，通过质量门限进行控制，以评估云服务产品的质量。所有云产品、云服务在发布前，均需完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。<br>3. 华为云定期会开展内部和第三方渗透测试和安全评估，监控、排查并解决安全威胁，保障云服务的安全性。<br>华为云参照ISO27001构建了信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性等。<br>1. 华为云安全技术团队，负责实施安全质量保证和安全评估，开展内部和第三方渗透测试和安全评估，监控、排查并解决安全威胁。 |

| | | | |
|---|---|---|---|
| | | | 2. 华为产品安全事件响应团队（ PSIRT – Product Security Incident Response Team ）已经建立成熟的漏洞响应机制，针对云的自运营的特点，通过持续优化安全漏洞的管理流程和技术手段，以保证基础设施、平台、应用和云服务中的自研和第三方漏洞尽快修复，降低对租户业务造成影响的风险。 |

| | | | |
|---|---|---|---|
| | | V - 根据这些领域的现有法规和最佳做法，建立业务连续性管理和变更管理程序；<br>VI - 制定灾难恢复计划，建立数据丢失事件后平台、基础架构，应用程序和数据的恢复和修复程序； | 在使用云服务时，客户应确认云服务提供商建立业务连续性管理机制及变更管理程序。<br>作为云服务提供商，华为云除提供高可用基础设施、冗余数据备份、可用区灾备等外，还制定业务连续性计划和灾难恢复计划，并定期对其进行测试。<br>**业务连续性管理：**华为云为向客户提供持续、稳定的云服务，华为云遵循ISO22301业务连续性管理国际标准的要求，建立了一套完善的业务连续性管理体系。在该体系框架的要求下，华为云定期开展业务影响分析、识别关键业务、确定关键业务的恢复目标及最小恢复水平。在识别关键业务的过程中，将业务中断对客户的影响程度作为判断关键业务的一个重要标准。<br>**变更管理流程：**华为云制定了完善的变更管理流程并定期对其评审和更新，按照变更可能对业务造成影响的程度定义了变更类别、变更窗口，并形成变更通告机制。该流程要求：在所有的变更申请生成后，由变更经理进行变更级别判断后提交给华为云变更委员会，通过评审后方可按计划对现网实施变更。所有的变更在申请前，都需通过类生产坏境测试、灰色发布、蓝绿部署等方式进行充分验证，使变更委员会能够清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响。<br>**灾难恢复计划：**华为云还制定了灾难恢复计划，并定期对其进行测试。例如，将一个地理位置或区域的云平台基础架构和云服务处于离线状态，模拟一个灾难，然后按照灾难恢 复计划进行系统处理和转移，以验证故障位置的业务及营运功能，测试结果将被 注释并记录归档，用以持续改进该计划。 |

| | | | |
|---|---|---|---|
| | | VII -至少使用安全套接字层/安全传输层（ SSL/ TLS ）建立安全通信通道； | 在使用云服务时，客户应确认云服务提供商使用安全套接字层/传输层（ SSL/ TLS ）建立安全通信通道。<br>华为云可以提 SSL/ TLS加密能力：<br>REST网络通道和 Highway 通道都支持TLS 1.2用于传输中的数据加密和基于X.509证书的目标网站身份验证。<br>1. **TLS能力：** 提供 REST 和 Highway 方式进行数据传输：<br>1. REST 网络通道是将服务以标准 RESTful 的形式向外发布，调用端直接使用。HTTP 客户端，通过标准 RESTful 形式对 API 进行调用，实现数据传输；<br>2. Highway 通道是高性能私有协议通道，在有特殊性能需求场景时可选用。上述两种数据传输方式均支持使用TLS 1.2 版本进行加密传输，同时也支持基于 X.509 证书的目标网站身份认证。<br>1. **SSL能力：** 证书管理服务（ SSL Certificate Service ）是华为云联合全球知名数字证书服务机构，为租户提供的一站式 X.509 证书的全生命周期管理服务，实现目标网站的可信身份认证与安全数据传输。 |

| | | | |
|---|---|---|---|
| | | VIII - 根据公认的国际标准，可以使用政府机构或实体生成并存储的加密密钥作为安全加密标准；<br>IX - 提供能够特定应用于政府机构或实体的加密保护的措施； | 在使用云服务时，客户应对数据进行加密管理，采用国际标准的加密算法和密钥管理机制对数据加密，并妥善保管相关密钥。<br>华为作为云提供商，为客户提供了数据加密服务（DEW）的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，确保了客户云上数据的安全。DEW采用分层密钥管理机制，方便各层密钥的轮换。华为云使用的硬件安全模块（HSM）为客户创建和管理密钥，HSM 拥有FIPS140-2（2级和3级）的主流国际安全认证，满足用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取客户根密钥。DEW还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业务的无缝集成、对接。同时，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机制，保障了密钥的持久性。 |

| | | | |
|---|---|---|---|
| | | X - 关于数据隔离：<br>（ a ）使用逻辑隔离方式，隔离其他云服务客户主体或实体的所有数据和服务；<br>（ b ）将流量管理流量与政府机构或实体流量进行隔离；和<br>（ c ）在区域之间实施安全装置； | 在使用云服务时，客户应确认云服务数据隔离能力。<br>华为云采用VPC等技术对云上租户的服务与数据进行隔离：<br>1. 华为云对云端数据的隔离是通过虚拟私有云（ VPC – Virtual PrivateCloud ）实现的，VPC 采用网络隔离技术，实现不同租户间在三层网络的完全隔离，云服务用户可以完全掌控自己的虚拟网络构建与配置：同时，利用 VPC 的访问控制列表 (ACL)、安全组功能，按需配置安全与访问规则，满足云租户更细粒度的网络隔离需要。<br>2. 为保证租户业务不影响管理操作，确保设备、资源和流量不会脱离有效监管，华为云将其网络的通信平面基于不同业务职能、不同安全风险等级和不同权限需要划分为租户数据平面、业务控制平面、平台运维平面、BMC（ Baseboard Management Controller ）管理平面、数据存储平面等，以保证关乎不同业务的网络通信流量得到合理且安全的分流，便于实现职责分离。<br>3. 华为云数据中心不同传统 IT 数据中心，因此在实现区域隔离上与传统手段不尽相同，不再是简单地使用防火墙实现，也会运用革新技术，如软件定义边界（ SDP – Software Defined Perimeter ）。并且，不止定义网络层区域边界，采用多层边界划分与隔离协防，从网络层、平台层、应用层一直到用户身份层，都有信任边界和相应的访问控制。 |

| | | | |
|---|---|---|---|
| | | XI - 制定与处置信息和数据资产有关的程序，确保：<br>（ a ）通过使用符合既定行为标准和最佳做法的方法，安全地清除或销毁废弃设备上的现有数据；<br>（ b ）在生命周期结束时或被认为无法使用时，安全销毁信息资产，并提供电子设备销毁证书（ CEED ），区分已回收的资产，以及因销毁而获得的材料的重量和类型；和<br>（ c ）以安全的方式将要丢弃的信息资产存储在具有受控物理访问的环境中，并记录设备输入和输出的所有动作； | 在使用云服务时，客户应确认云服务应制定处置信息和资产有关的程序。<br>华为云制定了介质管理程序，保障存储在介质中的数据的安全。当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循数据销毁标准和与客户之间的协议约定，对存储的客户数据进行清除。<br>实现方式如下：当客户确认删除操作后，华为云首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。<br>在生命周期结束时，华为云将对物理设备进行消磁，然后销毁物理设备。介质销毁后，华为可以提供销毁证书（ COD ），并获取废物分类和重量信息。 |
| | | XII - 针对提供的服务或在其监管下的数据发生的网络事件，应当立即通知政府机构或实体<br>； | 当发生网络事件时，云服务提供商应立即通知机构或实体。<br>华为云内部制定了完善的事件管理和客户通知通报流程。若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。根据内部的客户通知通报流程，在底层基础平台发生严重事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。 |

| | | | |
|---|---|---|---|
| | | XIII - 根据相关法规，建立保全证据所必需的程序；和 | 鉴于安全事件处理的专业性、紧迫性和可回溯性，华为云拥有完善的安全日志管理要求、安全事件定级处置流程和7*24小时的专业安全事件响应团队以及对应的安全专家资源池来应对。同时，华为云内部已根据法规要求建立了法证调查管理机制，制定了规范的取证流程，以支持安全事件的法证调查。 |
| | | XIV - 通过年度服务和组织控制 2（SOC 2）审计，由独立审计师进行，并提交 I类和 II类报告，证明符合云安全标准。 | 华为建立了专门的安全审计团队，审查全球安全法律法规及公司内部安全要求的遵从情况。审计团队每年投入10+人力对全球范围运营的华为云至少开展1次，为期2个月的审计，重点关注华为云在法律和流程遵从、业务目标达成、决策信息的可靠性、安全运维和安全运营上的风险。审计结果向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终闭环。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。<br>华为云完成了SOC审计项目，同时通过SOC 2 Type2五大控制属性（安全性、可用性 、进程完整性、保密性、隐私性），符合云安全标准。 SOC 2 Type II与SOC 2 Type I报告具有相同的意见，SOC 2 Type II比SOC 2 Type I增加了更多的运营有效性意见，以实现相关控制目标。<br>如有必要，政府机构可通过官方渠道向华为云申请SOC2 Type II审计报告副本。 |

| | | | |
|---|---|---|---|
| Art.22 | 使用云代理 | 如果机构或实体通过雇用云代理，使用多云管理平台来执行环境的预配和编排过程，则该平台工具必须至少具有：<br>I - 关于多云配置和编排功能：<br>（a）为最终用户提供单一的综合资源调配门户；<br>（b）配置模型的使用；<br>（c）同时提供和使用开源和可互操作工具的安全自动化；<br>（d）基于事件的编排工作流；和<br>（e）通过代码集成安全基础设施创建解决方案 – IaaC； | 华为云提供**华为云Stack**，Stack是位于政企客户本地数据中心的云基础设施，为政企客户提供在云上和本地部署体验一致的云服务。<br>ManageOne是华为云Stack方案中的多云管理平台，可为最终用户提供统一的综合资源调配门户，并提供自动作业（AutoOps）满足多云配置和编排功能。<br>自动作业是基于敏捷运维理念打造的运维自动化平台，提供基础架构到业务应用的全栈自动化运维能力。构建丰富的运维操作库，灵活编排运维流程，标准化各种运维场景，定时/立即批量执行运维操作或流程，可以根据企业的运维诉求按需扩展，最大限度的节约人力成本、降低管理风险、告别枯燥的重复工作，提升运维效率和满意度。<br>自动作业支持基础设施即代码IaaC。自动化执行的最小单位，由参数和脚本构成。将单个原子的运维脚本封装成一个运维操作，一个运维操作完成一个明确的运维动作，系统支持内置操作库和自定义操作库，内置操作库内置丰富的日常运维操作，自定义操作库方便用户按运维场景扩展自定义运维操作 |

| | | | |
|---|---|---|---|
| | | II - 关于多云监控和分析功能：<br>（a）监控云中资源性能的报告；<br>（b）收集和监控记录；和<br>（c）警报监控程序； | 华为云ManageOne多云管理平台，提供监控和分析功能：<br>1. **监控与分析：**可以通过监控仪表盘对告警、资源、应用等多方面的统计数据和健康状态。监控仪表盘可以实时集中监控容量、告警、资源等多方面的统计情况，同时提供丰富的图表组件和全面的运维数据，帮助运维人员通过自定义图表构建自定义监控，满足日常运维的需求。<br>2. **监控告警：**当出现告警或者异常时，能够快速识别风险，保障系统的正常运行。<br>3. **监控记录：**华为云ManageOne提供日志管理，由统一日志和ManageOne运维面日志管理组成，提供高效、安全的日志收集、查询、存储、下载、配置、管理等功能，帮助运维人员轻松应对日志采集、查询等运维场景。 |
| | | III - 关于多云资源和分类功能：<br>（a）云中的资源清单；<br>（b）在多云管理平台中配置资源的安全程序；和<br>（c）检测未标记的特征；和 | 华为云ManageOne多云管理平台，提供统一的资源管理中心：<br>1. **资源管理中心：**租户可通过资源中心快速的管理在云平台上申请的资源，支持按照多种维度查看资源，提高资源管理的效率。<br>2. **分类：**管理员通过定义不同的标签，并为资源绑定标签，将资源归类区分。标签是一种用来标记目标的分类或内容的工具，便于查找和定位目标。<br>3. **安全程序**：提供完善的安全控制机制，做到事前可定义安全策略，事中有安全提醒，事后可审计，避免人为的操作安全风险。 |

| | | | |
|---|---|---|---|
| | | IV - 关于安全性、合规性和身份管理功能：<br>（a）云平台的单点一多因素认证机制；<br>（b）安全管理用户和用户组；<br>（c）资源的安全管理；<br>（d）多渠道警报事件的通知；<br>（e）身份及认证管理–IAM；和<br>（f）云平台活动日志。 | 华为云ManageOne多云管理平台提供安全性、合规性和身份管理功能。<br>1. **身份管理：**在华为云Stack和华为云统一架构、统一IAM的基础上，ManageOne提供了混合云的新型实现，即云联邦混合云。云联邦混合云通过联邦认证和用户权限设置，实现了华为云Stack和华为云账号权限的一致性，使得华为云Stack VDC（Virtual Data Center）用户可以直接访问华为云控制台，使用华为云服务。云联邦混合云无需逐个 对接华为云服务，解决了传统混合云方案面临的问题。<br>2. **单点登录：**如果存在多个系统需要登录时，通过单点登录配置（SSO-Single Sign On），实现单点登录功能，用户成功登录服务端系统后，无须重复输入用户名和密码便可进入其他客户端系统。<br>3. **告警监控：**华为云提供告警监控功能，运维人员通过告警监控来监控、管理系统自身或管理对象上报的告警或事件。告警监控提供了丰富的监控和处理规则，还可以将故障通知给运维人员，帮助高效监控、快速定位和处理网络故障，从而保证业务正常运行。<br>4. **日志管理：**华为云ManageOne提供日志管理，由统一日志和ManageOne运维面日志管理组成，提供高效、安全的日志收集、查询、存储、下载、配置、管理等功能，帮助运维人员轻松应对日志采集、查询等运维场景。 |

| | | | |
|---|---|---|---|
| Art.25 | 一般规定 | SOC 2审计的 I 类和 II 类报告的呈现，证明符合云安全标准，是参与投标过程以及与联邦公共管理部门的机构或实体续签云服务交付合同的必备条件。 | 华为建立了专门的安全审计团队，审查全球安全法律法规及公司内部安全要求的遵从情况。审计团队每年投入10+人力对全球范围运营的华为云至少开展1次，为期2个月的审计，重点关注华为云在法律和流程遵从、业务目标达成、决策信息的可靠性、安全运维和安全运营上的风险。审计结果向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终闭环。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。<br>华为云完成了SOC审计项目，同时通过SOC 2 Type2五大控制属性（安全性、可用性 、进程完整性、保密性、隐私性），符合云安全标准。如有必要，政府机构可以通过官方渠道向华为云申请获取SOC 2审计报告的副本。 |

# 6 结语

华为云致力于为政府行业客户提供符合监管要求的安全的云环境，并持续改进华为云安全保障体系与安全能力以提高与政府监管标准的契合度。本文描述了华为云在政府监管重点领域下的安全实践，有助于政府行业客户详细了解华为云对于政府行业监管要求方面的遵从性，让客户安全、放心地使用华为云。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合政府行业监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

本白皮书仅供参考，不具备法律效应或构成法律建议。客户应酌情评估自身使用云服务的情况，并确保在使用华为云时对相关政府行业监管要求及其他适用法律的遵从性。

# 7 历史版本

| 日期 | 版本 | 描述 |
| --- | --- | --- |
| 2022年8月23日 | 1.0 | 首次发布 |