华为云 MPA 合规性说明——应用程序及云端分布式环境安全指南

文档版本 01

发布日期 2021-01-29

华为技术有限公司

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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 概述

1.1 适用范围

本文档提供的信息适用于华为云在中国站上开放的产品和服务。

1.2 发布目的

电影协会MPA（Motion Picture Association, Inc.）是全球电影、电视和流行媒体行业的主要倡导者，成员包括派拉蒙影业公司、索尼影视娱乐公司、环球影城有限责任公司、Netflix、迪士尼电影及华纳兄弟娱乐公司。其建立了一套安全存储、处理和传递受保护的媒体内容的最佳实践标准，包括《维护内容安全的最佳实践 - 通用指南》及《维护内容安全的最佳实践 –应用程序和云端分布式环境安全指南》。

为符合MPA对内容安全的期望和当前的行业最佳实践，华为云在本文档对《维护内容安全的最佳实践 –应用程序和云端分布式环境安全指南》各领域控制要求进行自评估，向客户展示华为云为提升内容安全性所做出的努力，帮助其了解：

- 《维护内容安全的最佳实践 –应用程序和云端分布式环境安全指南》的各领域主要的控制要求；
- 华为云针对于各领域控制要求所作出的回应。

1.3 基本定义

客户（租户）：指与华为云达成商业关系的注册用户，在本文中同租户含义一致，即使用华为云云服务的用户组织。

ISACA 国际信息系统审计协会：全球公认的信息科技管治、监控、保安，以及标准合规的领导组织。

SANS 系统管理、网络、安全研究院：世界上最受信任的信息安全培训和安全认证组织。SANS提供深入的沉浸式培训，旨在帮助企业及其员工掌握保护系统和网络免受最危险威胁所必需的实际步骤。

CSA 云安全联盟：一个致力于定义和提高对最佳实践认识的全球领先组织，帮助确保安全的云计算环境。

ISO 27001信息安全管理体系：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 27002 信息安全管理实践规范： ISO 27002是基于ISO 27001的最佳实践，同时也是MPA通用指南的官方映射标准。该标准根据各种准则和原则建立，用于在组织内启动、实施、改进和维护信息安全管理。

ISO 27017 云服务信息安全管理体系：基于ISO 27001体系框架与ISO 27002最佳实践的云服务信息安全控制的实用规则，是云服务信息安全控制实施规程的国际标准**。**

ISO 27018 公有云个人可识别信息（PII）管理体系：ISO 27018基于 ISO/IEC 信息安全标准ISO 27002，提供了适用于公有云个人信息的控制措施实施指导，旨在补充现有ISO27002 控制体系组合未能满足的公有云个人可识别信息（PII）保护要求。

ISO 22301 业务连续性管理体系：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。

CSA CCM云安全联盟云控制矩阵：世界上唯一的特定于云的安全控制元框架，框架映射到与安全、隐私等相关的领先的标准、最佳实践和法规。

SOC审计报告：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。

PCI DSS支付卡协会数据安全标准： 由VISA、JCB和万事达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，关于华为云的PCI DSS认证内容，请参考《华为云PCI DSS实践指南》。

NIST网络安全框架：NIST网络安全框架由标准、指南和管理网络安全相关风险的最佳实践三部分组成，其核心内容可以概括为经典的IPDRR能力模型，即风险识别能力（Identify）、安全防御能力（Protect）、安全检测能力（Detect）、安全响应能力（Response）和安全恢复能力（Recovery）五大能力。

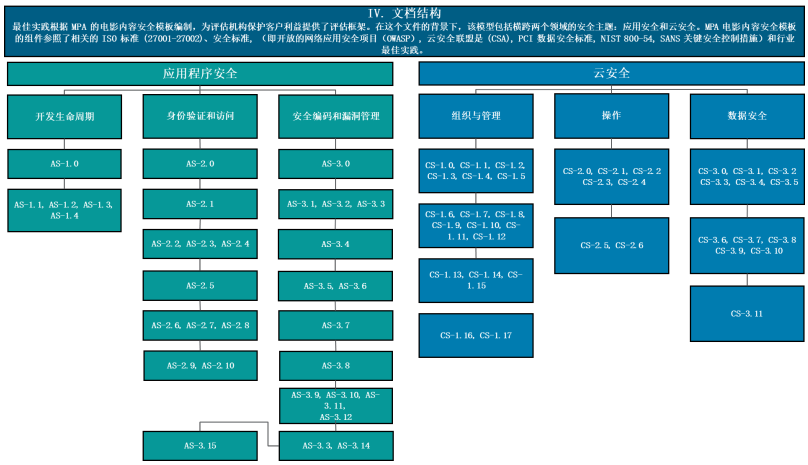
OWASP 开放式Web应用程序安全项目：一个非营利性基金会，致力于改善软件的安全性。通过社区主导的开源软件项目，全球数百个本地分会，数以万计的成员以及领先的教育和培训会议，OWASP 是开发人员和技术人员保护网络安全的来源。

2 MPA 简介

电影协会（Motion Picture Association, Inc.，简称 MPA）已成立超过30年，该协会前期以美国电影协会（Motion Picture Association of America, Inc.，简称 MPAA）命名，于2019年9月更名为电影协会（MPA），MPA致力于保护全球范围内为观众创造娱乐内容的公司及人员的权利，并建立了一套安全存储、处理和传递受保护的媒体内容的最佳实践标准。

MPA最佳实践包括《维护内容安全的最佳实践 - 通用指南》和《维护内容安全的最佳实践 –应用程序和云端分布式环境安全指南》，参照了相关的 ISO 标准、安全标准和行业最佳实践，阐述了最佳实践控制指南、实施步骤指导。

《维护内容安全的最佳实践 - 应用程序和云端分布式环境安全指南》由2个模块、6个安全主题、69个控制项组成，其参考标准包括：ISO 27001、ISO27002、OWASP、CSA、 PCI DSS、NIST 800-54及SANS。



在本文档中，华为云对《维护内容安全的最佳实践 - 应用程序和云端分布式环境安全指南》进行自评估，以满足MPA内容安全要求，并提升华为云在管理系统、物理安全、数字化内容安全等领域的管控能力。

3 华为云 MPA 评估表 - 维护内容安全的最佳实践 - 应用程序和云端分布式环境安全指南（V1.0）

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-1.0	开发生命周期	Build security into the entire Systems/ Software Development Lifecycle (SDLC).	通过结合华为在安全上的长期积累和华为云的现状，华为云不仅积极推行快速迭代的全新DevOps流程，还将华为的安全生命周期SDL无缝嵌入DevOps逐步形成高度自动化的DevSecOps全新安全生命周期管理流程，以及确保全新流程顺利而灵活执行的云安全工程能力和工具链 。	12.5 14.1	12.5 14	12.5 14	SOC1 6.1 SOC1 6.3 SOC1 6.4 SOC1 6.5 SOC1	AIS-01 AIS-02 AIS-03 AIS-04 BCR-01 CCC-03	6.1 6.2 6.3 6.4 6.5 6.6	SA-3 SA-4 SA-8 SA-11 SA-12

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-1.1	开发生命周期	Test security across the entire application and infrastructure.	所有云服务发布前都经过了多轮安全测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。详细可参考《华为云安全白皮书》。 同时，华为云将其深入 理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具，如 SecureCat 可以对业界主流的 OS 和 DB 的安全配置进行检查。				6.6			

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-1.2	开发生命周期	Perform fuzz testing and defect remediation to discover security loopholes in software, operating systems or networks by massive inputting of random data to the system in an attempt to make it crash (e.g., buffer overflow, cross-site scripting, denial of service attacks, format bugs, SQL injection).	华为云建立了攻击模式库，在云服务测试阶段均要通过攻击模式库测试，攻击模式库包含缓冲区溢出、跨站脚本、拒绝服务攻击、格式错误、SQL攻击等攻击模式。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-1.3	开发生命周期	Perform bug tracking and defect remediation in conjunction with extensive black box testing, beta testing, and other proven debugging methods.	所有云产品、云服务发布前都经过了多轮安全测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。详细可参考《华为云安全白皮书》。							
AS-1.4	开发生命周期	Provide training and user guides on additions and changes to the application.	在应用程序变更后，华为云会更新官网的使用指南，在使用过程中如有疑问，可联系华为云客服获取相应的支持。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.0	身份验证和访问	Implement secure authentication.	华为云的访问控制能力是通过统一身份认证服务IAM（Identity and Access Management）提供的。IAM是面向企业租户的安全管理服务，通过IAM，租户可以集中管理用户、安全凭证（例如访问密钥），以及控制用户管理权限和用户可访问的云资源权限，更多内容详见《华为云安全白皮书》。	9.1 9.2 9.3 9.4	9.1 9.2 9.3 9.4	9.1 9.2 9.3 9.4	SOC1 2.1 SOC1 2.2 SOC1 2.3 SOC1 2.4 SOC1 2.5 SOC1 4.3 SOC1 4.4 SOC1 4.5 SO	IAM-01 IAM-02 IAM-03 IAM-04 IAM-05 IAM-06 IAM-07 IAM-08 IAM-09 IAM-10	7.1 8.1 8.2	AC-2 AC-3 AC-6 AC-7 AC-8 AC-14 IA-5 IA-6 IA-8
AS-2.1	身份验证和访问	Register user devices.	所有运维帐号所有设备及应用的帐号均实现统一管理并通过统一审计平台集中控制，并且进行自动审计。以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。							
AS-2.2	身份验证和访问	Implement secure password recovery.	华为云为客户提供数据加密服务DEW，其支持密钥托管，可帮助客户轻松创建及管理密钥，基于DEW，客户可实现密钥的全生命周期管理。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.3	身份验证和访问	Follow the principle of least privilege.	华为云根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。登录权限分为：核心网络、接入网络、安全设备、业务系统、数据库系统、硬件维 护、监控维护等。不同岗位不同职责人员限定只能访问本角色所管辖的设备，其他设备无权访问。				C14.6 SOC14.7 SOC14.8	IAN-11 IAM-12 EKM-02 EKM-04 IVS-01		
AS-2.4	身份验证和访问	Implement controls to prevent brute force attacks.	IAM支持设定符合客户条件的账号锁定策略、账号停用策略及会话超时策略。在设置账号锁定策略后，在限定时间内登录失败次数到达设定值后，会将失败登录账号进行锁定，次数可在3~10次之间进行设置。IAM支持设置1~240天的非活动天数，若账号在设置天数内未登录，则被停用。并且在会话在设置时长范围内未进行操作，则需要重新登陆。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.5	身份验证和访问	Implement and document a process to secure key / cryptographic storage and ensure ongoing secure management.	华为云为客户提供数据加密服务DEW，DEW它可以提供专属加密、密钥管理、密钥对管理等功能。KMS 中所有密钥均由 HSM 的硬件真随机数生成器生成，保证密钥的随机性。KMS 的根密钥保存在 HSM 中，从来不会出现在 HSM 之外，确保根密钥不泄露。KMS 主机均使用标准的加密传输模式与 KMS 服务节点建立安全 通信链接，保证 KMS 相关数据在节点间的传输安全。KMS 基于 IAM 角色统一进行 RBAC 访问控制。对密钥的所有操作（例如创建用户主密钥、加密数据密钥等）， 都会产生日志并记录到云审计服务（CTS）中，便于后期审计。							
AS-2.6	身份验证和访问	Enable an auto-expiration setting to expire all external links to content after a user-defined time.	若会话在设置时长范围内未进行操作，则需要重新登陆，IAM支持最低15分钟的会话超时时长设置。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.7	身份验证和访问	Use human verification tools such as CAPTCHA or reCAPTCHA with web applications.	华为云为用户提供了云 Web 应用防火墙服务（WAF），华为云 WAF 可基于 IP、cookie和Referer 信息对用户进行标识，并通过灵活的配置阈值，执行访问限速，对超过阈值的访问者，可阻断其请求，避免对业务造成压力；也可发起验证码挑战，进行人机识别，更精准地将攻击者甄别出来，并进行阻断。							
AS-2.8	身份验证和访问	Provide clients with the ability to limit the number of times an asset may be downloaded or streamed by a particular user.	在华为云的部分服务中，可以限制客户对某个文件的权限（如浏览、下载、编辑等），以及限制客户权限的有效期。							
AS-2.9	身份验证和访问	Confirm the upload and download of all content and critical assets.	华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-2.10	身份验证和访问	Include a brief message on mobile applications to remind users to enable device passwords and to enable remote wipe and device location software.	移动设备可通过工作所需的华为云内部应用访问华为云企业办公环境，如及时沟通、邮件、论坛、人力管理 等，并为此建立了相应的规章制度。 但华为云不支持如IOS或安卓系统的手机、平板等移动设备对生产环境，尤其是客户内容数据的访问。							
AS-3.0	安全编码和系统	Perform penetration testing / web application security testing prior to production deployment, and at least quarterly thereafter. Validate vulnerabilities were remediated with a retest.	所有云服务发布前都经过了多轮安全测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。详细可参考《华为云安全白皮书》。华为云每季度都会组织内部以及外部具有一定资质的第三方进行对华为云的所有的系统、应用、网络进行漏洞扫描。并每半年聘请外部第三方对华为云的应用、网络进行渗透测试。	8.1 8.2 8.3 10.1 12.2 12.6 13.1 13.2	8.1 8.2 8.3 10.1 12.2 12.6 13.1 13.2	8.1 8.2 8.3 10.1 12.2 12.6 13.1 13.2	SOC1 3.4 SOC1 3.6 SOC1 10.4	STA-05 STA-09 AIS-03 IVS-01 SEF-02 SEF-05 DSI-03	1.2 1.3 1.4 5.1 5.2 5.3 10.6 11.1 11.2 11.3	AC-18 AU-5 CA-3 CA-9 SC-15 SC-18 SC-19

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.1	安全编码和系统	Perform vulnerability testing at least quarterly.	华为云每季度都会组织内部与第三方评估机构分别进行对华为云的所有的系统、应用、网络进行漏洞扫描，并每半年聘请外部第三方对华为云的应用、网络进行渗透测试。							SC-32 SC-7 SI-10 SI-11 SI-2 SI-3 SI-4 SI-8
AS-3.2	安全编码和系统	Utilize cookies in a secure manner (if they need to be used).	华为云制定适配当地要求的cookie政策，并部署 Web 应用防火墙应对 Web 攻击 ，包括攻击模式库的cookie注入等，以保护部署在DMZ区、面向外网的 Web 应用服务和系统 。							
AS-3.3	安全编码和系统	Validate user input and implement secure error handling.	数据完整性如SOC报告中所述，华为云制定了在数据生命周期所有阶段（包括传输、存储和处理）中维护数据的完整性控制的策略与程序，并定期依赖内部与外部审核来验证其有效性。 对于内容数据的完整性验证，客户需负责对华为云环境中使用的应用程序接口和数据库相关的数据输入输出校验控制的实现。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.4	安全编码和系统	Implement secure logging procedures.	华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，日志包含资源 ID(如源 IP、主机 ID 、用户 ID等、事件类型、日期时间、受影响的数据组件资源的ID（如目的 IP 、主机 ID 、服务 ID 等）、成功或失败等信息，以确保 支撑网络安全事件回溯和合规。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.5	安全编码和系统	Implement an SIEM (Security Information Event Management System) to aggregate and analyze the disparate logs.	华为云使用CLS日志系统对系统组件进行监控，收集并存储和分析所有系统组件日志，以及自主研发的CIP集中化安全事件管理系统分析安全事件并实时告警，系统基于威胁模型和专家定义规则进行智能分析。华为云也会定期对日志及安全事件的处理进行复核。 华为云针对关键基础设施、网络进行监控，可及时监测可能的网络攻击，避免数据泄露事件的发生。华为云建立了应对网络安全事件的响应流程，多个部门进行协同合作，及时监控事件，迅速部署处置措施，降低事件带来的影响。							
AS-3.6	安全编码和系统	Encrypt all content and client data at rest.	客户具有内容数据的所有权和控制权，负责其内容数据的质量以及承担数据质量带来的风险。 华为云使用密钥管理系统对加密密钥进行加密管理，数据加密密钥（DEK）及密钥加密密钥（KEK）的强度均为AES强效加密算法。 华为云的多个服务采用与密钥管理服务（DEW）集成的设计，方便客户管理密钥客户可以通过简单的加密设置，实现数据的存储加密。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.7	安全编码和系统	Encrypt all content and client data in transit.	华为云在网络传输过程中使用了业界通用的TLS高版本安全传输层协议及IPSec协议，在非信任网络之间传输敏感数据时使用安全传输通道或AES强效加密算法进行严格加密。							
AS-3.8	安全编码和系统	Implement controls for secure session management.	华为云参考业界会话安全设计的解决方案，针对会话管理中常见的漏洞及潜在风险，并结合公司现状，设计并实施会话生成、维持、销毁等管理控制机制。							
AS-3.9	安全编码和系统	Implement controls to prevent SQL injection.	华为云在开发服务时，将考虑各类可能的攻击，并设计开发相应的控制，在云服务测试阶段均要通过攻击模式库测试，攻击模式库包含缓冲区溢出、跨站脚本、拒绝服务攻击、格式错误、SQL 攻击等攻击模式等。							
AS-3.10	安全编码和系统	Implement controls to prevent unvalidated URL redirects and forwards.	华为云在开发服务时，将考虑各类可能的攻击，并设计开发相应的控制，在云服务测试阶段均要通过攻击模式库测试，攻击模式库包含缓冲区溢出、跨站脚本、拒绝服务攻击、格式错误、SQL 攻击等攻击模式等。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.11	安全编码和系统	Implement controls to prevent connections from anonymity networks (e.g., Tor, Freenet, Netshade), if possible.	华为云在开发服务时，将考虑各类可能的攻击，并设计开发相应的控制，在云服务测试阶段均要通过攻击模式库测试，攻击模式库包含缓冲区溢出、跨站脚本、拒绝服务攻击、格式错误、SQL 攻击等攻击模式等。							
AS-3.12	安全编码和系统	Implement controls to prevent IP address leakage.	华为云在开发服务时，将考虑各类可能的攻击，并设计开发相应的控制，在云服务测试阶段均要通过攻击模式库测试，攻击模式库包含缓冲区溢出、跨站脚本、拒绝服务攻击、格式错误、SQL 攻击等攻击模式等。							
AS-3.13	安全编码和系统	Implement controls to prevent XSS (Cross-site scripting).	华为云在开发服务时，将考虑各类可能的攻击，并设计开发相应的控制，在云服务测试阶段均要通过攻击模式库测试，攻击模式库包含缓冲区溢出、跨站脚本、拒绝服务攻击、格式错误、SQL 攻击等攻击模式等。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
AS-3.14	安全编码和系统	Allow senders the option to include session-based forensic (invisible) watermarking for content.	华为云不会对客户的内容数据的质量进行检查。华为云控制的数据质量及风险管控措施，可参见**《华为云数据安全白皮书》**。 客户具有内容数据的所有权和控制权，负责其内容数据的质量以及承担数据质量带来的风险。							
AS-3.15	安全编码和系统	Implement a formal, documented content / asset lifecycle.	华为云构建全数据生命周期的安全防护能力，通过自动化敏感数据发现、动态数据脱敏、高性能低成本数据加密、快速异常操作审计、数据安全销毁等多项技术的研究与应用，实现数据在创建、存储、使用、共享、归档、销毁等多个环节的管控，保障云上数据安全。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.0	组织与管理	Compliance with the MPA Content Best Practices Common Guidelines is required. Where stronger controls exist within the Application Security and Cloud/ Distributed Environment Guidelines, the stronger policy will prevail.	华为云已对MPA 内容最佳实践通用指南的要求进行自评估，具体的内容见本文档3.1。	5.1 6.1	5.1 6.1 7 8.2 10.1 12.1 15.1 16.1 CLD.8.1	5.1 6.1 7 8.2 10.1 12.1 15.1 16.1 A.4.1 A.9.1 A.9.3 A.10.1 A.10.7 A.10.12 A.10.13 A.11.1	SOC1 1.1 SOC1 1.2 SOC2 9.3 SOC2 9.4 SOC2 9.8 SOC2 10.1 SOC2 10.3 SOC2 10.4	GRM-03 AAC-01 AAC-02 GRM-01 HRS-03 STA-05 DSI-02 AIS-02 AIS-03 AIS-04 DSI-01	1.1 1.5 2.5 3.1 3.7 4.3 5.4 6.7 7.3 8.1 8.4 8.8 9.10 10 10.8 11.6 12.1 12.3 12.4	AC-1 AC-18 AC-19 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.1	组织与管理	Perform a third party security audit at least once per year (e.g., SSAE 16 Type 2, SOC 1, ISO 27000/27001, MPA).	华为云通过独立第三方对数据安全、隐私和安全进行审核，并取得认证，相关认证有：ISO27001、ISO27017、ISO27018、CSA STAR、ISO27701、ISO29151、SOC1/SOC2/SOC3、PCI DSS，相关证书或报告可以从**信任中心-合规性**获取，每年华为云都会请第三方对上述标准进行审核。					DSI-07 BCR-01 BCR-11 PCI-12 EKM-03 IAM-02 STA-07		RA-1 SC-1 SI-1
CS-1.2	组织与管理	Document and implement security and privacy policies that are aligned with security industry frameworks for Information Security Management (e.g., ISO-27001, ISO-22307, CoBIT).	根据ISO27001、ISO27701等标准的要求，华为云须发布和实施相应的安全和隐私政策。 每年华为云将请第三方对安全和隐私政策的有效性和实施情况进行审核。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.3	组织与管理	Document and implement information security baselines for every component of the infrastructure (e.g., Hypervisors, operating systems, routers, DNS servers, etc.).	华为云参考互联网安全中心CIS安全基线并将其融入华为云DevSecOps流程。CIS安全基线是一套用于网络系统安全配置和操作的业界优秀实践，覆盖技术（软件、硬件）、流程（系统和网络管理）、人员（最终用户和管理行为）。华为云建立内部的技术标准规范库，库中包含基础结构中各组件的信息安全基线。							
CS-1.4	组织与管理	Document and implement personnel security procedures that align with the organization’s current information security procedures.	ISO27001信息安全管理体系要求企业发布和实施符合组织当前的信息安全程序的人员安全程序，华为云已获得ISO27001信息安全管理体系认证，并且每年邀请第三方审核机构进行审核。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.5	组织与管理	Require all employees, contractors, and third parties to sign confidentiality / non-disclosure agreements when going through the onboarding process.	华为云的新雇用或已上岗的员工在授予员工用户访问公司设施、资源和资产的权限之前，需先签署雇佣合同以及保密协议，并完成信息安全相关培训。 供应商安全和隐私要求包含在已签署的合同协议中。与第三方的业务对接人员负责管理他们的第三方关系，包括资产保护要求和供应商对相关应用程序的访问。							
CS-1.6	组织与管理	Document and implement procedures for conducting security due diligence when offloading functionality or services to a third party.	华为云已建立供应商选择和监督体系，通过合同签订前的尽职调查以及合同签订后的定期评估来管理供应商对华为云具体的要求和合同义务的符合性。 华为云法务团队也会定期对合同的条款进行审查。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.7	组织与管理	Document and implement segregation of duties for business critical tasks.	华为云根据不同业务维度和相同业务不同职责，实行RBAC权限管理。登录权限分为：核心网络、接入网络、安全设备、业务系统、数据库系统、硬件维护、监控维护等。不同岗位不同职责人员限定只能访问本角色所管辖的设备，其他设备无权访问。							
CS-1.8	组织与管理	Provide clients with information regarding locations for their content and data.	客户在初次配置服务时可选择并决定内容数据存储的具体地理位置的可用区。 华为云不会在未通知客户的情况下从选定的地区移动客户的内容，除非为遵守法律或政府实体的要求所必须。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.9	组织与管理	Develop a documented procedure for responding to requests for client data from governments or third parties.	华为云会在提供服务之前和客户签订**《华为云用户协议》**、**《隐私政策声明》**、**《可接受的使用政策》**、《服务协议》、**《云服务等级协议（SLA）》**等，这些协议概述了服务要求的细则及双方的责任。 对于政府或者第三方提出的客户端数据要求，华为云会根据当地法律法规要求以及与客户的协议进行提供。 更多详细信息请查阅**《华为云安全白皮书》**。							
CS-1.10	组织与管理	Establish policies and procedures for labeling, handling, and securing containers that contain data and other containers.	ISO27001标准要求标识信息安全资产，华为云已通过ISO 27001认证，并为其信息安全资产建立清单和相应的管理程序。 客户是其内容数据的所有者和控制者，客户应对其内容数据的标签和处理建立相应的管控策略以确保数据的安全性。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.11	组织与管理	Establish procedures for the secure deletion of content/ data, including archived and backed-up content/ data.	华为云支持根据客户要求对数据进行安全删除，安全删除的方式包括删除加密存储的加密密钥、底层存储回收并覆写、对报废的物理介质进行消磁/折弯/粉碎。							
CS-1.12	组织与管理	Establish, document and implement scenarios to clients in which client content/ data may be moved from one physical location to another.	华为云已经通过ISO22301业务连续性管理体系标准的认证，在内部建立了业务连续性管理体系，并制定了业务连续性计划，其中包含了自然灾害、事故灾害、信息技术风险等突发事件的应对策略与应对流程。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.13	组织与管理	Establish, document and implement additional key management features, controls, policies and procedures.	ISO27001规定企业应建立和实施密钥管理的政策和程序，华为云建立了保护技术设备上数据的加密策略与密钥管理机制，包括人员的权限与职责分配、加密级别、加密方法进行了规定。 华为云为客户提供数据加密服务DEW，其支持密钥托管，可帮助客户轻松创建及管理密钥，基于DEW，客户可实现密钥的全生命周期管理。							
CS-1.14	组织与管理	Train personnel regarding all policies and procedures.	为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，华为从意识教育普及、宣传活动开展、 BCG及承诺书签署三个方面开展安全意识教育，详细可参考《华为云安全白皮书》。							
CS-1.15	组织与管理	Establish a process to notify clients when material changes are made to security/ privacy policies.	为保护最终用户和租户，华为云秉承负责任的披露原则，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。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-1.16	组织与管理	Plan, prepare and measure the required system performance to ensure acceptable service levels.	华为云在官网为客户提供SLA协议的内容，客户可查阅华为云**服务等级协议**页面获取更多信息。							
CS-1.17	组织与管理	Develop and maintain additional requirements for incident response and immediate notification to the client in the event of any unauthorized access to systems or content.	华为云建立了应对网络安全事件的响应流程，并针对关键基础设施、网络进行监控，可及时监测可能的网络攻击，避免数据泄露事件的发生。在华为云业务开展地区，若发生数据泄露事件，有专人负责通知客户及当地的监管部门。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-2.0	操作	Secure datacenter utilities services and environmental conditions.	华为云运维运营团队严格执行访问控制、安保措施、例行监控审计、应急响应等措施，以确保华为云数据中心的物理和环境安全，包括电力保障、温湿度控制、消防能力、例行监控、供水排水等，详情可见《华为云安全白皮书》。	11.1 11.2 11.5	8.1 11.1.1 12.1	8.1 11.1 12.1	SOC1 5.1 SOC1 5.3 SOC1 5.4 SOC1 5.5 SOC1 5.6 SOC1 5.7 SOC1 5.8 SOC1 5.9 SO	DCS-01 DCS-02 DCS-03 DCS-04 DCS-05 DCS-06 DCS-07 DCS-08 DCS-09 BCR-01 BC	1.1 1.5 2.5 3.1 3.7 4.3 5.4 6.7 7.3 8.1 8.4 8.8 9.2 9.4 9.10 10.8 11.6 12.1 12.3	PE-1 PE-18 PE-2 PE-3 PE-4 PE-5 PE-6 PE-8 PE-9 PL-8 PS-1
CS-2.1	操作	Ensure the data center has appropriate perimeter and physical security controls.	华为云数据中心采用当前通用的机房安保技术监测，并消除物理隐患。对机房外围、出入口、走廊、电梯、机房等进行7*24 小时闭路电视监控，并与红外感应、门禁等联动。保安人员对数据中心定时巡查，并设置在线巡更系统，详情可见《华为云安全白皮书》。							
CS-2.2	操作	Develop, document and maintain additional requirements for business continuity planning.	华为云已经通过ISO22301业务连续性管理体系标准的认证，在内部建立了业务连续性管理体系，并制定了业务连续性计划，其中包含了自然灾害、事故灾害、信息技术风险等突发事件的应对策略与应对流程。更多业务连续性相关的内容请查阅《华为云安全白皮书》。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-2.3	操作	Develop, document and maintain additional change and configuration controls.	华为云建立了系统的变更管理、服务上线流程，并将其要求传达给所有相关的开发人员（包含内部员工及外部合作伙伴），新上线或变更的服务应遵循华为云发布、变更管理流程的规定。				C15.10 SOC15.11 SOC15.12 SOC110.4	R-02 BCR-03 BCR-06 GRM-06		
CS-2.4	操作	Maintain a complete inventory of all critical assets, including ownership of the asset.	根据ISO27001标准，华为云的信息资产由专门的工具进行监控和管理，形成资产清单，每个资产均被指定所有者。华为云已通过ISO27001认证，认证证书可以从信任中心获取。							
CS-2.5	操作	Maintain an inventory of all critical supplier relationships.	华为云制定了供应商安全管理要求，定期对供应商进行审查，验证其是否符合华为云安全和隐私标准。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-2.6	操作	Develop and maintain service level agreements (SLA’s) with clients, partners, and service providers.	华为云在官网为客户提供SLA协议的内容，客户可查阅华为云**服务等级协议**页面获取更多信息。							
CS-3.0	数据安全	Implement a process to provide all relevant logs requested for good cause to clients in a format that can be easily exported from the platform for analysis in the event of a security incident.	华为云为客户提供了云审计服务（CTS），CTS可以记录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，更多信息可查阅《华为云安全白皮书》。	11.2 12.1	11.2 12.1 CLD.9.5 CLD.13.1	11.2 12.1 A.10.13	SOC1 3.1 SOC1 3.2 SOC1 3.3 SOC1 3.5 SOC1 3.6 SOC1	DSI-01 DSI-02 DSI-03 DSI-04 DSI-05 DSI-06 DSI-07	1.1 1.2 1.3 1.4 6.4 10.4 12.5	AC-3 AC-4 AC-5 AU-8 CA-3 CA-9 CM-6 CM-7 SC-19

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.1	数据安全	Consider providing the capability to use system geographic location as an additional authentication factor.	华为云IAM按层次和细粒度授权，通过密码认证、多因子认证、联邦认证等方式对用户进行权限管理。				3.9 SOC1 3.10 SOC1 3.11 SOC1 3.12 SOC1 3.13 SOC1 3.14 SOC1 3.15 SOC1 3.16 SOC1 7.1			SC-5 SC-7 SI-4
CS-3.2	数据安全	Provide the capability to control the physical location/ geography of storage of a client’s content/ data, if requested.	客户在初次配置服务时可选择并决定内容数据存储的具体地理位置的可用区。 华为云不会在未通知客户的情况下从选定的地区移动客户的内容，除非为遵守法律或政府实体的要求所必须。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.3	数据安全	Establish procedures to ensure that non-production data must not be replicated to production environments.	华为云对于生产及非生产环境使用物理和逻辑控制并用的隔离手段，控制并用的隔离手段，提升网络面对入侵和内部违规操作的分区自我保护和容错恢复能力。				SOC1 7.2 SOC1 7.3 SOC1 7.4 SOC1 7.5 SOC1 7.6 SOC1 7.7 SOC1 7.8 SOC1 10.4			

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.4	数据安全	Establish, document and implement a published procedure for exiting the service arrangement with a client, including assurance to sanitize all computing systems of client content/ data once the client contract has terminated.	在客户内容数据的销毁阶段，华为云会对指定的数据及其所有副本进行全面的清除。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 。 华为云支持客户对账户进行注销。当客户提出账户注销的申请并通过华为云对账号的验证后，客户内容数据进入保留期，保留期内，客户不能访问及使用云服务，但对客户存储在云服务中的数据仍予以保留。保留期届满后，客户内容数据会得到彻底的清除，无法进行恢复。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.5	数据安全	Establish and document policies and procedures for secure disposal of equipment, categorized by asset type, used outside the organization’s premises.	对于物理存储介质报废，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。							
CS-3.6	数据安全	Implement a synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference.	华为云使用NTP4.2.8协议对系统内的时间进行同步。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.7	数据安全	Design and configure network and virtual environments to restrict and monitor traffic between trusted and untrusted connections.	华为云根据业务功能和网络安全风险，通过物理和逻辑控制将生产网络划分为DMZ区、公共服务区、资源交付区、数据存储区、运维管理区，其中资源交付区提供租户所需的基础设施资源，包括计算、存储、网络资源，如租户虚拟机、磁盘、虚拟网络。租户之间通过多层安全控制手段实现资源隔离，租户不能访问其它租户的资源；平台侧管理 平面、数据存储平面隔离，且与租户数据平面隔离。该区域还可以支撑对进出互 联网的租户流量做 DDoS 防护及入侵检测与防御，保障租户业务。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.8	数据安全	Design, develop and deploy multi-tenant applications, systems, and components such that client content and data is appropriately segmented.	华为云承载了众多客户的数据，各服务产品和组件从设计之初就规划并实现了隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。 华为云对云端数据的隔离是通过虚拟私有云VPC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。							
CS-3.9	数据安全	Use secure and encrypted communication channels when migrating physical servers, applications, and content data to/ from virtual servers.	云数据迁移服务CDM（Cloud Data Migration）在用户VPC中运行，通过网络隔离确保数据传输的安全性。支持SSL的数据源，如RDS、SFTP等，可以使用SSL。CDM还支持公网数据源的数据上云，用户可以利用VPN和SSL技术来避免传输安全风险。 用户数据源的访问信息（用户名和密码）存储在CDM实例的数据库中，并采用AES-256加密。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.10	数据安全	Implement technical measures and apply defense-in-depth techniques (e.g., deep-packet analysis, traffic throttling, black-holing) for detection and timely response to network-based attacks associated with unusual ingress/ egress traffic patterns (e.g., NAC spoofing and ARP poisoning attacks and/or DDOS attacks).	华为云为提升云服务的安全性，应用多种高级防护功能保护内网区域，包括DDoS异常和超大流量清洗、网络入侵检测与拦截、Web安全防护。详细可参考《华为云安全白皮书》。							

NO.	安全主题	最佳实践	华为云的回应	ISO 27002	ISO 27017	ISO 27018	SOC	CSA CCM	PCI DSS	NIST 800-53
CS-3.11	数据安全	Establish and document controls to secure virtualized environments.	华为统一虚拟化平台UVP（Unified Virtualization Platform）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。在中国可信云认证中，华为云平台的云主机获得最高级的五星认证 。							

4 结语

华为云始终秉持着华为公司“以客户为中心”的核心价值观，积极践行信息安全实践，为此华为云构建了信息安全管理体系，应用业界通用的信息安全保护技术，通过第三方机构的认证与审核检查安全控制的有效落实，致力于保护客户的数据安全。

同时，为帮助客户应对日益复杂和开放的网络环境及日益发展的信息安全技术，华为云不断开发各种数据保护领域的工具、服务和方案，支持客户提升数据保护能力，降低风险。

本白皮书仅供客户作为参考，不具备任何法律效力或构成法律建议，也不作为任何客户在云上环境一定合规的依据。客户应酌情评估自身业务和安全需求，选用适合的云产品及服务。

5 版本历史

日期	版本	描述
2021年01月	1.0	首次发布