华为云 MPA 合规性说明通用指南

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 – 通用指南》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 – 通用指南》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。

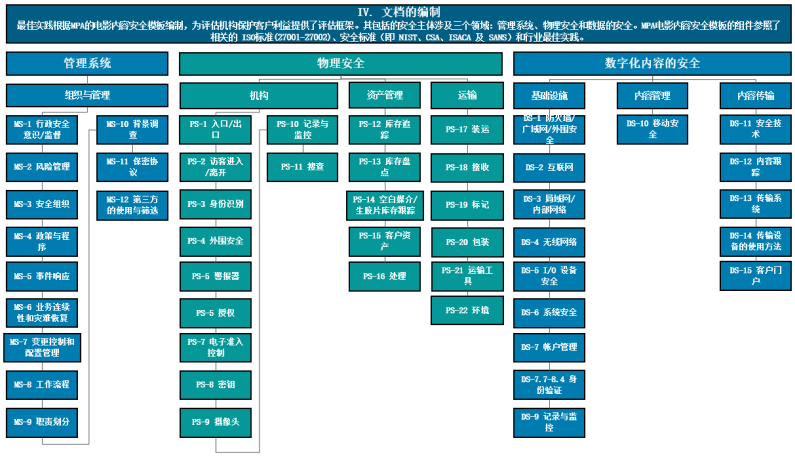
OWASP 开放式Web应用程序安全项目：一个非营利性基金会，致力于改善软件的安全性。通过社区主导的开源软件项目，全球数百个本地分会，数以万计的成员以及领先的教育和培训会议，OWASP 是开发人员和技术人员保护网络安全的来源。

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 – 通用指南》由3个模块、7个安全领域、49个安全主题、261个控制项组成，其参考标准包括：ISO 27001、ISO27002、NIST、CSA、ISACA 及 SANS；



在本文档中，华为云对《维护内容安全的最佳实践 – 通用指南》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 - 通用指南（V4.08）

3.1 MS 管理系统

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
MS-1.0	行政安全意识/监管	Establish an information security management system that implements a control framework for information security which is approved by the business owner(s)/ senior management.	华为云已建立信息安全管理体系，该信息安全管理体系已通过ISO27001认证。作为ISO/IEC 27001 ISMS认证 的一部分，信息安全相关的角色和职责通过书面的方式确定并获得高级领导层的审批。 华为云通过独立第三方对数据安全、隐私和安全的审核，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。	5.1.2 6.1.1	5.1.1 7.2.2		SOC1 1.1 SOC1 1.2 SOC2 9.1	GRM-02 GRM-05 GRM-06 GRM-09 AAC-02 AAC-03	12.1 12.4 12.5	AT-2 AT-3 PM-1 PM-2 PM-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
MS-1.1	行政安全意识/监管	Review content/ information security management policies and processes at least annually. Policies must be approved by senior management.	ISO27001信息安全管理体系要求至少每年审查一次信息安全管理策略和流程，政策及流程的变更需要获得高级管理层的审批。华为云已经通过ISO27001认证，且每年都会邀请第三方独立认证机构进行审查。							
MS-1.2	行政安全意识/监管	Train and engage executive management/ owner(s) on the business' responsibilities to protect content at least annually.	华为云建立了自己的培训机制，对不同的角色设计合适的培训方案，一般员工至少每年进行一次培训，以提升其信息保护意识，核心岗位员工培训频率比一般员工高。							

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
MS-1.3	行政安全意识/监管	Create an information security management group to establish and review information security management policies.	华为云依据ISO27001及SOC2的要求，实施文档化的信息安全政策和程序，为华为云的操作和信息安全管理提供指导。员工可根据授权查看已发布的信息安全政策和程序。							
MS-2.0	风险管理	Develop a formal, documented security risk assessment process focused on content workflows and sensitive assets in order to identify and prioritize risks of content theft and leakage that are relevant to the facility.	华为云已经实施了一个正式的、有文件记录的风险评估政策，该政策至少每年更新和审查一次。 风险评估的目的是识别华为云的威胁和漏洞，基于业务流程和资产管理情况，为威胁和脆弱性分配风险评级，正式记录评估，并为解决问题制定风险处理计划。	5.1.2 6.1.1			SOC1.2 SOC2 9.3	GRM-02 GRM-08 GRM-10 GRM-11 TVM-02	12.1 12.2	CA-1 RA-1 RA-2

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
MS-2.1	风险管理	Conduct an internal security risk assessment annually and upon key workflow changes—based on, at a minimum, the MPA Best Practice Common Guidelines and the applicable Supplemental Guidelines—and document and act upon identified risks.	华为云每年进行风险评估，包括识别关键流程更新可能存在的数据安全风险，根据已识别的风险采取行动。风险评估报告完成后将会获得高级管理层的审批。在审计SOC、PCI DSS、ISO 27001等合规性期间，华为云风险管理框架由独立外部审计师进行审查。 客户保留对其内容数据的所有权，并负责评估和管理与其数据相关的风险，以满足其法规遵从性需求。							

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
MS-3.0	安保组织	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection.	华为云在《华为云安全白皮书》中通过责任共担模型，阐述了华为云作为云服务提供商与客户分别承担的安全管理责任。 华为云根据不同角色、岗位制定相应的安全基础能力培训计划。新员工转正前必须通过有关网络安全与隐私保护的上岗培训和考试；在岗员工需根据不同业务角色，选择相应课程进行学习与考试。管理者需参加网络安全必须的培训和研讨。 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，ISO27001信息安全管理体系的审核中也包含了此部分要求。	6.1.3			SOC1.1	HRS-07	12.4 12.5	PM-2

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
MS-4.0	政策与程序	Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum: Acceptable use (e.g., social media, Internet, phone, personal devices, mobile devices, etc.) Asset and content classification and handling policies Business continuity (backup, retention and restoration) Content transfer	ISO27001信息安全管理体系要求企业建立包含资产和内容安全等相关政策和流程，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。	5.1.1 5.1.2 6.1.1 8.1.3 8.2.2	7.2.2 12.3.1	A.10.3	SOC1 1.2 SOC2 9.1 SOC2 9.4	MOS-05 BCR-01 DSI-01 BCR-11 AAC-01 AAC-02 HRS-09	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 10.8 11.6 12.1 12.3 12.4	AT-1 AT-2 AT-3 AT-4 PL-1 PS-7

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
		processes and systems Change control and configuration management policy Confidentiality policy Digital recording devices (e.g., smart phones, digital cameras, camcorders) Exception policy (e.g., process to document policy deviations) Incident response policy Mobile device policy Network, internet and wireless policies								

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
		Password controls (e.g., password minimum length, screensavers) Security policy Visitor policy Disciplinary/ Sanction policy Internal anonymous method to report piracy or mishandling of content (e.g., telephone hotline or email address)								
MS-4.0.1	政策与程序	Establish dedicated policies governing the use of social media by company personnel.	华为云制定社交媒体相关政策，禁止在办公网络中私自启用互联网服务，员工无法通过华为内网访问社交媒体。							

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
MS-4.0.2	政策与程序	Establish policies governing the using of mobile computing devices.	华为云对移动设备安全管理建立制度规定，并每年邀请第三方审核机构对该制度的适用性进行审核，该制度包含对移动计算机设备的管理要求。							
MS-4.1	政策与程序	Review and update security policies and procedures at least annually.	ISO27001信息安全管理体系要求至少每年审查一次信息安全管理策略和流程，并根据需要予以更新，以反映业务目标或风险环境的变更情况。政策及流程的变更需要获得高级管理层的审批。华为云已经通过ISO27001认证，且每年都会邀请第三方独立认证机构进行审查。							

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
MS-4.2	政策与程序	Communicate and require sign-off from all company personnel (e.g., employees, temporary workers, interns) and third party workers (e.g., contractors, freelancers, temp agencies) for all current policies, procedures, and/or client requirements.	将网络安全纳入《华为员工商业行为准则》（BCG –Business Conduct Guide），通过公司统一开展的年度例行 BCG 学习、考试和签署活动来传递公司对全员在网络安全领域的要求，提高员工网络安全意识。签署网络安全承诺书，承诺遵守公司各项网络安全政策和制度要求。							

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
MS-4.3	政策与程序	Develop and regularly update an awareness program about security policies and procedures and train company personnel and third party workers upon hire and annually thereafter on those security policies and procedures, addressing the following areas at a minimum: IT security policies and procedures Content/ asset security and	华为云员工入职时须参加入职培训，入职培训中包含信息安全内容，在职期间，员工会每年参加信息安全培训，年度的信息安全培训都会被计划、实施和监督。 华为云通过多种培训方式进行信息安全意识培训，所有的员工都需要完成年度培训，培训记录可以证实所有人员已经阅读和理解了信息安全政策。签署网络安全承诺书，员工承诺遵守公司各项网络安全政策和制度要求。							

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
		handling in general and client-specific requirements Social media policies Social engineering prevention Security incident reporting and escalation Disciplinary policy Encryption and key management for all individuals who handle encrypted content Asset disposal and destruction processes								

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
MS-5.0	事件响应	Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported.	华为云参照ISO27001建立信息安全管理体系，其中包含事件响应流程和计划。另外，华为云制定了安全事件响应操作的内部规范，明确云安全事件的定级及通报机制、处理流程及人员职责。	16.1.1 16.1.2		A9.1	SOC18.1 SOC18.2	BCR-01 SEF-01 SEF-02 SEF-03	10.6 12.1	IR-1 IR-2 IR-4 IR-5 IR-6 IR-7 IR-8
MS-5.1	事件响应	Identify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents.	华为云参照ISO27001标准建立信息安全管理体系，其中包含事件响应流程和计划。华为云也建立了安全事件响应团队，要求流程中各角色人员履行其对应职责。							

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
MS-5.2	事件响应	Establish a security incident reporting process for individuals to report detected incidents to the security incident response team.	华为云建立ISO27001信息安全管理体系，其中包含事件响应流程和计划，安全事件可通过多个渠道通知到事件响应团队成员。							

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
MS-5.2.1	事件响应	Anonymous reporting should be made available to organizations with 50 or more employees and third party personnel for reporting of content protection and privacy concerns. The anonymous reporting tool consisting of an internal, anonymous telephone number, email address, and / or website should be published and also provided during security	华为云员工入职时须参加入职培训，入职培训时会告知员工进行匿名举报的途径。 第三方人员入场前需完成信息安全培训，并在培训中会告知其安全事件匿名举报途径。							

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
		awareness training.								
MS-5.3	事件响应	*(Removed and combined with MS-5.2)*	N/A							
MS-6.0	业务连续性和灾难恢复	Establish a formal plan that describes actions to be taken to ensure business continuity.	华为云已经通过ISO22301业务连续性管理体系认证，在内部建立了业务连续性管理体系，并制定业务连续性计划，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。	17.1.1			SOC1 8.1 SOC1 8.2 SOC2 10.3	BCR-01 BCR-02 BCR-05 BCR-08 BCR-10 BCR-11		CP
MS-6.1	业务连续性和灾难恢复	Identify the business continuity team who will be responsible for detecting, analyzing and remediating continuity incidents.	华为云已经通过ISO22301业务连续性管理体系认证，在内部建立了业务连续性管理体系，制定了业务连续性管理规定，组建业务连续性响应团队并定义其岗位职责。华为云也对定期测试业务连续性计划的有效性。							

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
MS-6.2	业务连续性和灾难恢复	Establish a data backup policy that addresses the following: Systems and data Retention and protection requirements Backup frequency Encryption Recovery time objectives (RTO) Recovery point objectives (RPO) Restoration testing Secure offsite storage	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，在业务连续性管理体系中要求华为云建立数据备份策略，以解决系统及数据的可用性问题。更详细的内容参考《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
MS-7.0	变更控制和配置管理	Establish policies and procedures to ensure new data, applications, network, and systems components have been pre-approved by business leadership.	华为云设置配置经理对所有业务单元进行配置管理，包括提取配置模型（配置项类型、各类配置项属性、配置项间的关系等），记录配置信息等。并通过专业的配置管理数据库工具CMDB(Configuration Management Database)，对配置项、配置项的属性和配置项之间的关系进行管理。 华为云的各项变更都是影响云服务运行的因素。生产环境各要素如机房设施、网络、系统平台软硬件和应用等的更改，包括设备增减、架构调整、系统软件更新（含网络系统，操作系统镜像和应用容器）、配置改变等发生变更，都需要通过有序的活动进行变更管理。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。	14.2.2	12.1.2		SOC1 6.1	CCC-01 CCC-03 CCC-04 CCC-05 GRM-01	6.4	CM

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
MS-8.0	工作流程	Document workflows tracking content and authorization checkpoints. Include the following processes for both physical and digital content: Delivery (receipt/ return) Ingest Movement Storage Removal/ destruction	保护内容数据的工作流文档是华为云客户的责任，因为客户保留对其客户操作系统、软件、应用程序和数据的所有权和控制权。	11.1						
MS-8.1	工作流程	*(Removed and combined with MS-8.0)*	N/A							

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
MS-9.0	职责划分	Segregate duties within the content workflow. Implement and document compensating controls where segregation is not practical.	华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。 华为云为客户提供的虚拟私有云（VPC）服务可为租户构建出私有网络环境，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，并通过配置网络ACL和安全组规则，对进出子网和虚拟机的网络流量进行严格的管控，满足租户更细粒度的网络隔离需求。 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，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。 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。	6.1.2				IAM-01 IAM-02 IAM-03 IAM-05 IAM-06		

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
MS-10.0	背景检查	Perform background screening checks on all company personnel, third party workers, and their relevant subcontractors.	华为云要求机要岗位、关键岗位员工上岗前需进行背景调查，接口部门视业务需要对外部人员进行背景调查。	7.1.1			SOC2 9.5	HRS-02	12.7	PS-3
MS-11.0	保密协议	Require all company personnel to sign a confidentiality agreement (e.g., non-disclosure) upon hire and review annually thereafter, that includes requirements for handling and protecting content.	员工入职时，签署的聘用协议中含保密条款，机要岗位员工还需签署相关NDA。员工还需签署网络安全承诺书，员工承诺遵守公司各项网络安全政策和制度要求。	7.1.2 8.1.4		A.10.1		HRS-01 HRS-06		PL-4 PS-6 PS-8 PS-4 PS-6 PS-8 SA-9

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
MS-11.1	保密协议	Require all company personnel to return all content and client information in their possession upon termination of their employment or contract.	华为云制定了人员安全相关的管理规定，要求员工离职或离岗时向公司移交所持有的华为云的资产。与合作伙伴合同/业务关系终止时，合作伙伴将按照合作协议删除自带设备中在合作项目中产生的信息，并退还华为云提供的资产。							
MS-12.0	第三方使用与筛选	Require all third party workers (e.g., freelancers) who handle content to sign confidentiality agreements (e.g., non-disclosure) upon engagement.	对于外部人员，接口部门需要与其所属组织签署保密协议，若合作事项涉及敏感信息，与外部人员加签保密协议。	7.1.1 7.1.2 7.2.1 8.1.4 11.1.2	16.1.1 16.1.2	A.7.1	SOC15.11 SOC15.12	DCS-02 DCS-07 DCS-09 IVS-11	2.6 12.6 12.8 12.9	PL-4 PS-4 PS-6 PS-7 SA-9

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
MS-12.1	第三方使用与筛选	Require all third party workers to return all content and client information in their possession upon termination of their contract.	华为云要求在合作终止时，对于外部人员自带设备中包含的在合作项目中产生的信息，接口部门应按照合作协议予以处置，如果涉及公司敏感信息的，应予以回收或销毁。							
MS-12.2	第三方使用与筛选	Include security requirements in third party contracts.	华为云依据ISO27001的要求管理第三方供应商，并与其签署保密及**服务水平协议**，协议中包含安全和隐私数据处理的要求。与供应商签订的合同需要经过多轮合同评审流程，合同内容由华为云法务团队负责审查。							
MS-12.3	第三方使用与筛选	Implement a process to reclaim content when terminating relationships with third party service providers.	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。 华为云要求在合作终止时，对于外部人员自带设备中包含的在合作项目中产生的信息，接口部门应按照合作协议予以处置，如果涉及公司敏感信息的，应予以回收或销毁。							

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
MS-12.4	第三方使用与筛选	Require third party workers to be bonded and insured where appropriate (e.g., courier service).	华为云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。							
MS-12.5	第三方使用与筛选	Restrict third party access to content / production areas unless required for their job function.	华为云依据ISO27001的要求管理第三方供应商，并与其签署保密及服务水平协议，协议中包含安全和隐私数据处理的要求，管理其访问权限不应超过其服务所必须。同时，华为云通过门禁控制系统，严格审核包括第三方在内的人员出入权限。							
MS-12.5.1	第三方使用与筛选	Control access of third party IT service providers to the computing environment.	华为云为第三方人员提供单独的账号，在入职前依据其工作职责与工作内容，依据权限最小化原则为其提供权限，包含对权限范围内的数据、应用程序、基础架构、网络组件的访问。							

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
MS-12.6	第三方使用与筛选	Notify clients if third parties are used to handle or store content, or work is offloaded to another company. Perform due diligence of third parties. Third parties also include providers of IT services. Obtain client approval for use of third parties who handle, store, or have access to content.	华为云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。							

3.2 PS 物理安全

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
PS-1.0	入口/出口	Secure all entry/exit points of the facility at all times, including loading dock doors and windows.	华为云已制定并实施完善的物理和环境安全防护策略、规程和措施，满足GB50174《电子信息机房设计规范》A类和TIA942《数据中心机房通信基础设施标准》中的T3标准。华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略，严格审核人员出入权限。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。对非法闯入和其他安保事件及时进行声光报警。	11.1			SOC15.1 SOC15.6	DCS-02 DCS-06 DCS-07 DCS-09	9.1	PE-1 PE-2 PE-3 PE-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
PS-1.1	入口/出口	Control access to areas where content is handled by segregating the content area from other facility areas (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication and mastering).	华为云数据中心不但有妥善的选址，在设计施工和运营时，合理划分了机房物理区域，合理布置了信息系统的组件，以防范物理和环境潜在危险。 数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置了全天候一天 24 小时、一周 7 天，即 7* 24 小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。							

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
PS-1.2	入口/出口	Control access where there are collocated businesses in a facility, which includes but is not limited to the following: • Segregating work areas • Implementing access-controlled entrances and exits that can be segmented per business unit • Logging and monitoring of all entrances and exits within facility • All tenants within the facility must be reported to client	华为云与数据中心运营商签署管理合同，要求运营商负责数据中心的日常运营管理。 华为云严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。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。华为云通过合同与运营商协定安全策略，同时运营商对不同租户进行物理隔离，以防止未授权访问。							

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
		prior to engagement								
PS-2.0	访客进入/离开	Maintain a detailed visitors' log and include the following: • Name • Company • Time in/ time out • Reason for visit • Person/ people visited • Signature of visitor • Badge number assigned	访客进入数据中心之前需要进行申请，进入数据中心时需要进行登记，访客日志包括访客名字、公司、时间、访客签名等。	11.1			SOC1 5.1 SOC1 5.4	IAM-04 DCS-09	9.1 9.2 9.4	PE-2 PE-3 PE-7
PS-2.1	访客进入/离开	Assign an identification badge or sticker which must be visible at all times, to each visitor and collect badges upon exit.	访客进入数据中心时需要获取并佩戴访客牌，访客离开时退还访客牌。							

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
PS-2.2	访客进入/离开	Do not provide visitors with key card access to content / production areas.	在华为云人员出入安全管理规定中要求访客在数据中心现场或内容/生产区域须由授权员工陪同。							
PS-2.3	访客进入/离开	Require visitors to be escorted by authorized employees while on-site, or in content / production areas.	在华为云人员出入安全管理规定中要求访客在数据中心现场或内容/生产区域须由授权员工陪同。							
PS-2.3.1	访客进入/离开	Visitors should be required to sign a nondisclosure agreement (NDA) and sign a visitor log prior to entering a facility.	华为云要求数据中心内部人员在上岗前应签署保密协议，与运营商签订的管理合同要求数据中心运营人员应遵守保密协议，一般的数据中心来访人员需要数据中心内部人员全程陪同，并且只能在一般限制区域活动。							

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
PS-3.0	身份识别	For organizations with 25 or more employees and third-party workers, provide company personnel and long-term third party workers (e.g., janitorial) with a photo identification badge that is required to be visible at all times.	华为云对数据中心人员和长期第三方员工执行身份管理，员工出入门禁系统均须使用本人身份识别徽章区分门禁权限。	11.1.2			SOC1 5.1	DCS-09	9.1 9.2 9.4	PE-3

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
PS-4.0	外围安全	Implement perimeter security controls that address risks that the facility may be exposed to as identified by the organization's risk assessment.	华为云已制定并实施完善的物理和环境安全防护策略、规程和措施，满足GB50174《电子信息机房设计规范》A类和TIA942《数据中心机房通信基础设施标准》中的T3标准。华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。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。对非法闯入和其他安保事件及时进行声光报警。	11.1.1			SOC1 5.1 SOC1 5.4	DCS-02	9.1	PE-3

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
PS-4.1	外围安全	Place security guards at perimeter entrances and non-emergency entry/ exit points.	华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。保安人员对数据中心定时巡查，并设置在线巡更系统。对非法闯入和其他安保事件及时进行声光报警。同时，华为云也在办公环境周边入口和各关键出入境点设立保安站岗看守。							
PS-4.2	外围安全	Implement a daily security patrol process with a randomized schedule and document the patrol results in a log.	华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。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。对非法闯入和其他安保事件及时进行声光报警。							

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
PS-4.3	外围安全	Lock Perimeter gates at all times.	华为云已制定并实施完善的物理和环境安全防护策略、规程和措施，满足GB50174《电子信息机房设计规范》A类和TIA942《数据中心机房通信基础设施标准》中的T3标准。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。							
PS-5.0	警报器	Install a centralized, audible alarm system that covers all entry/exit points (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/ machine room, etc.).	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。对非法闯入和其他安保事件及时进行声光报警。 数据中心部署了自动报警和自动灭火系统，能够迅速准确发现并通报火情。自动报警系统与供电、监控 、通风设备联动，即使意外情况造成无人值守，也能开启自动灭火系统得以控制火情。	11.1.1			SOC15.1 SOC15.3 SOC15.6 SOC15.7	DCS-02 DCS-07 IAM-02 IAM-04 IAM-05 IAM-10	9.1	AC-6 PE-3 PE-6 PE-9 PE-10 PE-11 PE-13

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
PS-5.1	警报器	Install and effectively position motion detectors in restricted areas (e.g., vault, server/ machine room) and configure them to alert the appropriate security and other personnel (e.g. project managers, producer, head of editorial, incident response team, etc.).	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小时闭路电视监控及移动侦测报警，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。对非法闯入和其他安保事件及时进行声光报警 。							

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
PS-5.2	警报器	Install door prop alarms in restricted areas (e.g. vault, server, machine rooms) to notify when sensitive entry/exit points are open for longer than a pre-determined period of time (e.g., 60 seconds).	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小时闭路电视监控及移动侦测报警，并与红外感应、门禁等联动，保安定时巡查各敏感出入口，以及时确认出入口打开的异动情况。							
PS-5.3	警报器	Configure alarms to provide escalation notifications directly to the personnel in charge of security and other personnel (e.g., project managers, producer, head of editorial, incident response team, etc.).	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。对非法闯入和其他安保事件及时进行声光报警 。							

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
PS-5.4	警报器	Assign unique arm and disarm codes to each person that requires access to the alarm system and restrict access to all other personnel.	华为云内部的IAM系统负责对数据中心员工全生命周期的管理，对其的身份信息、职位、访问权限、账号类别进行存储与管理。							
PS-5.5	警报器	Review the list of users who can arm and disarm alarm systems quarterly, or upon change of personnel.	华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。员工的登陆、操作等日志将留存需要的时间以响应审核需求。							
PS-5.6	警报器	Test the alarm system 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。							

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
PS-5.7	警报器	Implement fire safety measures so that in the event of a power outage, fire doors fail open, and all others fail shut to prevent unauthorized access.	华为云对电气、消防安全执行严格管控。华为云数据中心采用多级保护方案保障业务7*24小时持续运行，日常电力供应采用来自不同变电站的双路市电供电。配备柴油发电机，在市电断电时可启动柴油机供电，以备不时之需。并配备了不间断电源(UPS Uninterrupted Power Supply)，提供短期备用电力供应。 华为云数据中心建筑防火等级均按一级设计施工，使用了A级防火材料，满足国家消防规范。采用了阻燃、耐火电缆，在管内或线槽铺设，并设置了漏电检测装置。部署了自动报警和自动灭火系统，能够迅速准确发现并通报火情。自动报警系统与供电、监控、通风设备联动，即使意外情况造成无人值守，也能开启自动灭火系统得以控制火情 。							

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
PS-6.0	授权	Document and implement a process to manage facility access and keep records of any changes to access rights.	华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。员工的登陆、操作等日志将留存需要的时间以响应审核需求。	11.1			SOC 15.1 SOC 15.3	IAM-02 IAM-05 IAM-10 IVS-08	9.1 9.2 9.4	PE-2 PE-3
PS-6.1	授权	Restrict access to production systems to authorized personnel only.	华为云对接入主机操作系统的华为云管理员执行严格的权限访问控制，对其所执行的各项运维运营操作实行全面的日志审计。 华为云管理员必须经过双因子认证后，才能通过堡垒机接入管理平面，所有操作都会记录日志并及时传送到集中日志审计系统。							

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
PS-6.2	授权	Review access to restricted areas (e.g., vault, server/ machine room) quarterly and when the roles or employment status of company personnel and/or third party workers are changed.	华为云依据员工工作需要为其提供所需的最小权限，并定期对权限进行审阅，使系统用户及管理员的始终遵循最小权限原则。 员工及其他第三方在状态发生变化后，如离职或职位变更后，按照调动、离职安全审查清单，对内部调离、离职人员进行离岗安全审查，包括离岗权限账号的清理或修改等。							
PS-7.0	电子接入控制	Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or processed.	华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置了全天候一天24小时、一周7天，即7* 24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。 华为云对员工按工作需要的最小范围分配权限，并对其信息安全管理系统、敏感信息的访问、修改等操作进行监控和记录。	11.1			SOC1 5.1 SOC1 5.3	DCS-02	9.1 9.2 9.4	PE-2 PE-3

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
PS-7.1	电子接入控制	Restrict electronic access system administration to appropriate personnel.	IAM系统负责对数据中心员工全生命周期的管理，对其的身份信息、职位、访问权限、账号类别进行存储与管理。华为云将该系统限制由指定人员进行管理，以实现职责分离。 华为云对每个API请求通过与华为云IAM的集成进行身份验证，确保只有经过身份验证的用户才能访问和管理云监控信息，且传输通道通过TLS 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
PS-7.2	电子接入控制	Store card stock and electronic access devices (e.g., keycards, key fobs) in a locked cabinet and ensure electronic access devices remain disabled prior to being assigned to personnel. Store unassigned electronic access devices (e.g., keycards, key fobs) in a locked cabinet and ensure these remain disabled prior to being assigned to personnel.	华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置了全天候一天24小时、一周7天，即7* 24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。 华为云对员工按工作需要的最小范围分配权限，并对其信息安全管理系统、敏感信息的访问、修改等操作进行监控和记录。							

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
PS-7.3	电子接入控制	Disable lost electronic access devices (e.g., keycards, key fobs) in the system before issuing a new electronic access device.	华为云的内部管理规定要求员工在确认丢失工卡时及时应向安全岗登记。华为云内部规定卡办理流程，对员工电子接入设备进行统一管理，包括设备的激活、发放、回收和权限撤销。							
PS-7.4	电子接入控制	Issue third party access electronic access devices with a set expiration date (e.g. 90 days) based on an approved timeframe.	分配给第三方员工的电子接入设备会设定设备到期时间，要求电子接入设备到期时进行回收，并执行权限撤销操作。							

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
PS-8.0	密钥	Limit the distribution of master keys and / or keys to restricted areas to authorized personnel only (e.g., owner, facilities management).	华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。员工的登陆、操作等日志将留存需要的时间以响应审核需求。	9.2.6 11.1			SOC1 5.1	DCS-02 HRS-01	9.1	PE-2 PE-3 CM-5 CM-8
PS-8.1	密钥	Implement a check-in/check-out process to track and monitor the distribution of master keys and / or keys to restricted areas.	数据中心机房门禁或有关钥匙持有权限，应由机房管理员或数据中心门禁管理员向数据中心大区经理或其授权的数据中心站点经理申请，通过门禁权限申请流程方可发放相应钥匙。							
PS-8.2	密钥	Use keys that can only be copied by a specific locksmith for exterior entry/exit points.	数据中心机房门禁或有关钥匙持有权限，应由机房管理员或数据中心门禁管理员向数据中心大区经理或其授权的数据中心站点经理申请，通过门禁权限申请流程方可发放相应钥匙。							

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
PS-8.3	密钥	Inventory master keys and keys to restricted areas, including facility entry/exit points, quarterly.	华为云依据员工工作需要为其提供所需的最小权限，并定期对权限进行审阅，使系统用户及管理员始终遵循最小权限原则。							
PS-8.4	密钥	Obtain all keys from terminated employees/third-parties or those who no longer need the access.	华为云制定了人员安全相关管理规定，要求员工离职或离岗时向公司移交所持有的华为云资产。与合作伙伴合同/业务关系终止时，按照合作协议删除自带设备中在合作项目中产生的信息，并移交华为云提供的资产。 华为云建立了人员离职/合作终止时的资产交接电子流，按照电子流程执行资产交接。							
PS-8.5	密钥	Implement electronic access control or rekey entire facility when master or sub-master keys are lost or missing.	数据中心对钥匙的使用管理进行规定，包括钥匙分类，钥匙存放要求以及钥匙丢失后的补偿措施等。 对于电子访问控制，华为云依据ISO27001的要求建立访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。							

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
PS-9.0	摄像头	Install a surveillance camera system (analog CCTV or IP cameras) that records all facility entry/exit points and restricted areas (e.g. server/ machine room, etc.).	华为云已制定并实施完善的物理和环境安全防护策略、规程和措施，满足GB50174《电子信息机房设计规范》A类和TIA942《数据中心机房通信基础设施标准》中的T3标准。 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。对非法闯入和其他安保事件及时进行声光报警。	11.1				DCS-02 BCR-05 IAM-01 IAM-04 IAM-05	9.1	PE-2 PE-3 CM-5 CM-8
PS-9.1	摄像头	Review camera positioning and recordings to ensure adequate coverage, function, image quality, lighting conditions, and frame rate of surveillance footage at least daily.	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，并且有专门的团队对CCTV进行管理，维护CCTV的正常运行。							

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
PS-9.2	摄像头	Restrict physical and/or logical access to the surveillance camera console and to camera equipment (e.g., DVRs, NVRs) to personnel responsible for administering/ monitoring the system.	华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。员工的登陆、操作等日志将留存需要的时间以响应审核需求。 由专人定期对所有物理访问设备和仓储系统物资进行综合盘点追踪。机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，避免非授权人员访问数据中心。							

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
PS-9.3	摄像头	Ensure that camera footage includes an accurate date and time-stamp and retain camera surveillance footage and electronic access logs for at least 90 days, or the maximum time allowed by law, in a secure location.	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。 华为云制定数据中心安全防范规范，要求对各区域的监控录像保留超过90天。							
PS-9.4	摄像头	Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected security incidents.	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。对非法闯入和其他安保事件及时进行声光报警。同时，指定安保人员在监控各区域摄像情况，对发现的安全事件进行及时上报。							

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
PS-10.0	记录与监控	Log and review electronic access to restricted areas for suspicious events, at least weekly.	华为云对员工按工作需要的最小范围分配权限，并对其信息安全管理系统、敏感信息的访问、修改等操作进行实时监控和记录。	10.1 12.4			SOC 15.1 SOC 15.4	BCR-05 IVS-02 SEF-05	9.1	AU-3 AU-6 AU-9 AU-11
PS-10.1	记录与监控	Log and review electronic access, at least daily, for the following areas: • Masters/ stampers vault • Pre-mastering • Server/ machine room • Scrap room • High-security cages	华为云对员工按工作需要的最小范围分配权限，并对其信息安全管理系统、敏感信息的访问、修改等操作进行实时监控和记录。							

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
PS-10.2	记录与监控	Investigate suspicious electronic access activities that are detected.	华为云对提供的服务的网络设备、应用系统启用安全日志，日志对设备、系统的所有更改都会进行记录。 华为云为客户提供各类服务帮助客户进行日志记录和监控，客户可使用云日志服务对虚拟机的配置、日志的更改进行记录，使用云审计服务对于配置的日志的完整性进行监控。 客户可使用企业主机安全（HSS）服务对镜像文件进行完整性校验，对比的方法来确定当前文件状态是否不同于上次扫描该文件时的状态，利用这种对比来确定文件是否发生了有效或可疑的修改。当发现潜在风险，将及时提醒客户。							
PS-10.3	记录与监控	Maintain an ongoing log of all confirmed electronic access incidents and include documentation of any follow-up activities that were taken.	华为云建立了事件管理平台，用于记录和跟踪所有的信息安全事件的进展、处置措施与落实，对事件处置后的影响进行分析。 华为云提供多类安全服务产品，租户根据自身业务情况进行配置后，通过安全服务产品进行相关的安全事件监控与数据收集。							

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
PS-11.0	搜查	Establish a policy, as permitted by local laws, which allows security to randomly search persons, bags, packages, and personal items for client content.	华为云内部制定物理安全规范，在当地法律允许情况下严格执行检查措施。	11.1				BCR-05 STA-01 IVS-08		

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
PS-11.1	搜查	Implement an exit search process that is applicable to all facility personnel and visitors, including: • Removal of all outer coats, hats, and belts for inspection • Removal of all pocket contents • Performance of a self-pat-down with the supervision of security • Thorough inspection of all bags • Inspection of laptops' CD/DVD tray • Scanning of individuals	华为云内部制定物理安全规范，在当地法律允许情况下严格执行检查措施。							

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
		with a handheld metal detector used within three inches of the individual searched.								
PS-11.2	搜查	Prohibit personnel from entering/ exiting the facility with digital recording devices (e.g., USB thumb drives, digital cameras, cell phones) and include the search of these devices as part of the exit search procedure.	华为云内部制定物理安全规范，在当地法律允许情况下严格执行检查措施。							

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
PS-11.3	搜查	Enforce the use of transparent plastic bags and food containers for any food brought into production areas.	华为云内部制定物理安全规范，在当地法律允许情况下严格执行检查措施。							
PS-11.4	搜查	Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts).	华为云内部制定物理安全规范，在当地法律允许情况下严格执行检查措施。							
PS-11.5	搜查	Use numbered tamper-evident stickers/ holograms to identify authorized devices that can be taken in and out of the facility.	华为云内部制定物理安全规范，严格执行检查措施。							

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
PS-11.6	搜查	Implement a process to test the exit search procedure.	华为云建立了一个正式的、定期的审计计划，包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以验证华为云控制环境的实施和运行有效性。							
PS-11.7	搜查	Perform a random vehicle search process when exiting the facility parking lot.	为规范化出入安全管理，华为云制定车辆出入及停放相关管理规定，对车辆出入规定区域进行严格管控。							
PS-11.8	搜查	Segregate replication lines that process highly sensitive content and perform searches upon exiting segregated areas.	数据中心不但有妥善的选址，在设计施工和运营时，合理划分了机房物理区域（包括高度敏感区域），合理布置了信息系统的组件，以防范物理和环境潜在危险。 华为云要求来访者需内部人员全程陪同，并且只能在一般限制区域活动。							

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
PS-11.9	搜查	Implement additional controls to monitor security guards activity.	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。 机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，从而使非授权人员不可访问数据中心。							
PS-12.0	库存跟踪	Implement a content asset management system to provide detailed tracking of physical assets (i.e., received from client created at the facility).	华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，为用户提供最切实有效的数据保护能力，保证租户对其数据的隐私权、所有权和控制权不受侵犯。	8.1 8.2.2 8.2.3	8.1.1			DSI-01 BCR-05 IVS-01	9.9	AU-1 AU-3 AU-6 AU-9 AU-11 CM-8

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
PS-12.1	库存跟踪	Assign unique tracking identifier(s) to client assets and create media (e.g., tapes, hard drives) upon receipt and store assets in the vault when not in use.	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。							
PS-12.1.1	库存跟踪	Develop a data classification scheme to categorize physical assets of differing security requirements. *(Reordered and renumbered, previously PS-12.1.2)*	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。							
PS-12.2	库存跟踪	Retain asset movement transaction logs for at least one year.	华为云建立资产管理系统管理资产的移动和交易，保留相应记录，记录的保留时间符合当地法律法规的要求。							

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
PS-12.3	库存跟踪	Review logs from content asset management system at least weekly and investigate anomalies.	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。 华为云有专门的内审部门，定期对运维流程各项活动日志进行审计。对于日志的访问和审核权限只限于特定员工，其权限的审批需收到上级管理人员的批准，并定期进行审核。							
PS-12.4	库存跟踪	Use studio film title aliases on physical assets and in asset tracking systems.	根据ISO27001标准，华为云的信息资产分类由专门的工具进行监控和管理，形成资产清单，每个资产均有唯一的资产编号。							
PS-12.5	库存跟踪	Implement and review a daily aging report to identify highly sensitive assets that are checked out from the vault and not checked back in.	根据ISO27001标准，华为云的信息资产分类由专门的工具进行监控和管理，形成资产清单，每个资产均有唯一的资产编号。							

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
PS-12.5.1	库存跟踪	A documented process for checking out content should be established.	华为云严格遵循ISO27001信息安全管理体系中关于设备的条款A11.2要求，采取控制措施防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断，并每年对此要求的落实进行审计。							
PS-12.6	库存跟踪	Lock up and log assets that are delayed or returned if shipments could not be delivered on time.	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。							
PS-13.0	库存盘点	Perform a quarterly inventory count of each client's asset(s), reconcile against asset management records, and immediately communicate variances to clients.	根据ISO27001标准，华为云的信息资产分类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。	6.1.2 8.1.1				DCS-01 STA-01		AU-6 AC-5 CM-8

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
PS-13.1	库存盘点	Segregate duties between the vault staff and individuals who are responsible for performing inventory counts.	华为云制定介质管理标准，对存储介质的物理保护和库存控制进行规定，要求至少一名没有直接参与介质方面的工作人员参加库存盘点，以遵循职责分离的原则。							
PS-14.0	空白媒介/生胶片库存跟踪	Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per unit when received.	根据ISO27001标准，华为云的信息资产分类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。	8.1.1 8.2.2				STA-01		MP-4 PE-2 PE-3
PS-14.1	空白媒介/生胶片库存跟踪	Establish a process to track consumption of raw materials (e.g., polycarbonate) monthly.	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。 同时，云监控服务（CES Cloud Eye Service）为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。							

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
PS-14.2	空白媒介/生胶片库存跟踪	Store blank media/raw stock in a secured location.	华为云制定介质管理标准，要求存储介质必须保存在受控访问区，所有存储介质都必须纳入介质管理流程来管理。 对于数据中心的重要配件，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；对于数据中心的任何配件，都必须提供授权工单方能领取，且领取时须在仓储管理系统中登记。由专人定期对所有物理访问设备和仓储系统物资进行综合盘点追踪。							
PS-15.0	客户资产	Restrict access to finished client assets to personnel responsible for tracking and managing assets.	数据中心合理划分机房物理区域，客户的数据保存在数据中心的生产区域。 华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。员工的登陆、操作等日志将留存需要的时间以响应审核需求。	8.2.3			SOC15.1 SOC15.4	IAM-02 STA-01 BCR-05 DCS-07	9.1 9.9	MP-2 MP-4 PE-2 PE-3

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
PS-15.1	客户资产	Store client assets in a restricted and secure area (e.g., vault, safe, or other secure storage location).	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。对非法闯入和其他安保事件及时进行声光报警 。							
PS-15.2	客户资产	Consider requiring two company personnel with separate access cards or keys / pins to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours.	华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。员工的登陆、操作等日志将留存需要的时间以响应审核需求。							
PS-15.3	客户资产	Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight.	在物理保护方面，华为云设立了分区防护；对于可能的自然灾害制定了选址策略以消减风险；对于入侵、授权等风险，建立了监控机制及响应机制。							

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
PS-15.4	客户资产	Implement a dedicated, secure area (e.g., security cage, secure room) for the storage of undelivered screeners that is locked, access-controlled, and monitored with surveillance cameras and/or security guards.	客户在对华为云服务进行配置时，可自主选择专用的数据中心。 华为云数据中心合理划分机房物理区域，客户的数据保存在数据中心的生产区域。 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。对非法闯入和其他安保事件及时进行声光报警 。							

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
PS-16.0	处理	Require that rejected, damaged, and obsolete stock (DVDs, tapes, and other storage media) containing client assets are erased, degaussed, shredded, or physically destroyed before disposal.	当物理磁盘报废时，华为云通过物理方式清除存储介质中的数据，并对数据清除操作保存完整记录，满足行业标准，使用户隐私和数据不受未授权访问 。	8.3.2	11.2.7	A.9.3 A.10.13		DCS-05 DCS-07 IAM-05	9.8	MP-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
PS-16.0.1	处理	Finished elements (e.g., check discs, test prints, mock-ups, ADR scripts) should be destroyed immediately after use, unless otherwise specified by content owners. Require paper materials containing client assets (scripts, artwork, storyboards, etc.) be physically destroyed before disposal.	华为云制定相关介质管理规定，其中对介质清退报废进行分类操作，通过多种方式实现数据清除，磁盘消磁，并记录销毁操作。 当物理磁盘报废时，华为云通过物理方式清除存储介质中的数据，并对数据清除操作保存完整记录，满足行业标准，使用户隐私和数据不受未授权访问 。							

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
PS-16.1	处理	Store elements targeted for recycling / destruction in a secure location / container to prevent the copying and reuse of assets prior to disposal.	华为云对废弃工程辅料采取本地报废的处置方式，当物理磁盘报废时，华为云通过物理方式清除存储介质中的数据，并对数据清除操作保存完整记录，满足行业标准，使用户隐私和数据不受未授权访问 。							
PS-16.2	处理	Maintain a log of asset disposal for at least 12 months.	华为云建立资产管理系统管理资产的移动和交易，保留相应记录，记录的保留时间符合当地法律法规的要求。							

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
PS-16.3	处理	Destruction must be performed on site. On site destruction must be supervised and signed off by two company personnel. If a third party destruction company is engaged, destruction must be supervised and signed off by two company personnel and certificates of destruction must be retained.	华为云对存储介质的物理保护和库存控制进行规定，要求消磁操作在摄像头覆盖下进行，或有2人同时在场，其中1人必须是数据中心经理或其指定人员。消磁后的介质要做好明显标识，并保留消磁记录。							

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
PS-16.4	处理	Use automation to transfer rejected discs from replication machines directly into scrap bins (no machine operator handling).	华为云业务中的介质不涉及光盘。当物理磁盘报废时，华为云通过物理方法清除存储介质中的数据，并对数据清除操作保存完整记录，满足行业标准，使用户隐私和数据不受未授权访问 。							
PS-17.0	装运	Require the facility to generate a valid work/ shipping order to authorize client asset shipments out of the facility.	客户具有内容数据的所有权和控制权，华为云根据和客户的约定接收和管理客户的资产。	8.2.3 8.3.3		A.10.4		STA-01 DCS-02 DCS-04	9.9	AU-11 MP-5 PE-3 PE-7 PE-16

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
PS-17.1	装运	Track and log client asset shipping details; at a minimum, include the following: • Time of shipment • Sender name and signature • Recipient name • Address of destination • Tracking number from courier Reference to the corresponding work order	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。							
PS-17.2	装运	Secure client assets that are waiting to be picked up.	华为云数据中心对机房物理区域进行划分，其中设置交接区，通过特定控制对客户资产进行安全防护。							

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
PS-17.3	装运	Validate client assets leaving the facility against a valid work/ shipping order.	客户具有内容数据的所有权和控制权，华为云根据和客户的约定接收和管理客户的资产。							
PS-17.4	装运	Prohibit couriers and delivery personnel from entering content / production areas of the facility.	华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。							
PS-17.5	装运	Document and retain a separate log for truck driver information.	数据中心园区门岗对进入园区的车辆、人员、物品进行登记检查并保留相关记录。							
PS-17.5.1	装运	Facilities should implement and maintain a record of all delivery personnel entering and exiting the building.	数据中心园区门岗对进入园区的车辆、人员、物品进行登记检查并保留相关记录。							

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
PS-17.6	装运	Observe and monitor the on-site packing and sealing of trailers prior to shipping.	数据中心园区门岗对进入园区的车辆、人员、物品进行登记检查并保留相关记录。							
PS-17.7	装运	Record, monitor and review travel times, routes, and delivery times for shipments between facilities.	华为云数据中心进行7*24 小时闭路电视监控，并与当地第三方快递公司签订运输合同，由第三方快递公司负责包裹的装载。							
PS-17.8	装运	Prohibit the transfer of film elements outside of the shipping department unless approved by the client.	华为云业务不涉及薄膜原件的转移							

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
PS-17.9	装运	Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels).	华为云业务不涉及提供用于电影放映的印刷品。							
PS-18.0	接收	Inspect delivered client assets upon receipt and compare to shipping documents (e.g., packing slip, manifest log).	客户具有内容数据的所有权和控制权，华为云根据和客户的约定接收和管理客户的资产。	8.2.2 8.2.3				STA-01	9.9	MP-3 MP-4 MP-5 PE-16
PS-18.1	接收	Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries.	数据中心园区门岗对进入园区的车辆、人员、物品进行登记检查并保留相关记录，华为云根据和客户的约定维护接收日志。							

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
PS-18.2	接收	Perform the following actions immediately: • Tag (e.g., barcode, assign unique identifier) received assets • Input the asset into the asset management system • Move the asset to the restricted area (e.g., vault, safe)	华为云收到资产时为资产分配唯一的标识符，将资产输入管理系统，并将资产存储至指定的区域。如未使用的资产会放在专门的库房，数据中心的重要配件由仓储系统中的专门电子加密保险箱存放，存放了数据的下架资产会放在保险柜。							
PS-18.3	接收	Implement a secure method for receiving overnight deliveries.	在适用情况下，根据客户要求接收客户资产。							

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
PS-19.0	标记	Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages unless instructed otherwise by client.	根据ISO27001标准，华为云的信息资产分类由专门的工具进行监控和管理，形成资产清单，每个资产均有唯一的资产编号，资产编号与客户无关，用于维护资产管理清单。	8.2.2	8.2.2			DSI-04	9.9	MP-3
PS-20.0	包装	Ship all client assets in closed/ sealed containers, and use locked containers depending on asset value, or if instructed by the client.	在适用情况下，对客户的资产按照客户要求进行包装。	8.3.3						MP-5

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
PS-20.1	包装	Implement at least one of the following controls: • Tamper-evident tape • Tamper-evident packaging • Tamper-evident seals (e.g., in the form of holograms) • Secure containers (e.g., Pelican case with a combination lock).	在适用情况下，对客户的资产按照客户要求进行包装。							
PS-20.2	包装	Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped.	在适用情况下，对客户的资产按照客户要求进行包装。							

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
PS-21.0	运输工具	Lock automobiles and trucks at all times, and do not place packages in clear view.	华为云与当地第三方快递公司签署运输合同，由第三方快递公司负责包裹的装载。					STA-01		MP-5
PS-21.1	运输工具	Include the following security features in transportation vehicles (e.g., trailers): • Segregation from driver cabin • Ability to lock and seal cargo area doors • GPS for high-security shipments	华为云与当地第三方快递公司签署运输合同，由第三方快递公司负责包裹的装载。							
PS-21.2	运输工具	Apply numbered seals on cargo doors for shipments of highly sensitive titles.	华为云与当地第三方快递公司签署运输合同，由第三方快递公司负责包裹的装载。							

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
PS-21.3	运输工具	Require security escorts to be used when delivering highly sensitive content to high-risk areas.	华为云与当地第三方快递公司签署运输合同，由第三方快递公司负责包裹的装载。							
PS-22.0	环境	Maintain optimal temperature and humidity set-points to facilitate optimal performance of equipment and to reduce the likelihood of catastrophic hardware failures for areas that house servers, storage devices, LAN equipment, network communications devices, and storage media.	通过精密空调、集中加湿器自动调节华为云数据中心机房温湿度保持在设备运行所允许的范围内使设备元器件处于良好运行状态。机柜冷热通道有合理的布置，利用架空地板下空间作为静压箱来给机柜送风，并设置了冷通道密闭，以防止局部热点。	11				BCR-03		

3.3 DS 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
DS-1.0	防火墙 / 广域网 / 周边安全	Separate external network(s)/ WAN(s) from the internal network(s) by using inspection firewall(s) with Access Control Lists that prevent unauthorized access to any internal network and with the ability to keep up with upload and download traffic.	华为云对云平台安全区域进行划分，通过使用Anti-DDoS, IPS, WAF等多层防护， 实现内部与外部的网络隔离。	9.1 9.4 10.1 12.2 12.3 12.4 12.6 13.1 13.2 16.1 17.1	9.4.1 10.1.1 12.4.4 12.6.1 13.1.3		SOC1 3.1 SOC1 3.4 SOC1 5.15 SOC1 8.1	IVS-03 IVS-06 IVS-07 IVS-08 IVS-11 IVS-12 AIS-01 BCR-11 TVM-02 CCC-03 GRM-01	1.1 1.2 1.3 1.4 5.1 5.2 5.3 10.1 10.2 10.3 10.4 11.2 11.3 12.5	AC-3 AC-4 AC-6 AC-17 AC-20 CA-3 CM-6 CM-7 RA-5 SC-7 SC-12 SC-33 SI-2

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
DS-1.1	防火墙 / 广域网 / 周边安全	Implement a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the business every 6 months.	华为云有专业的网络安全团队负责网络体系结构图的更新，并对各区域之间的防火墙规则进行检查。在华为云PCI DSS认证的年度审查中，该项内容也会通过第三方机构进行审计。所有防火墙的控制及变更记录均被记录至安全日志中，防火墙配置需要特定管理员审批后才可变更。					EKM-02 EKM-03		

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
DS-1.1.1	防火墙 / 广域网 / 周边安全	Firewall management policies and procedures must be documented, and at a minimum, cover: • Provisioning requirements (i.e., based off the concept of least-privilege) • Deployment requirements (e.g., baseline requirements) • Change control requirements (e.g., Patching, Upgrades, Firewall Rule management)	所有防火墙的控制及变更记录均被记录至安全日志中，防火墙配置需要特定管理员审批后才可变更。 租户负责部署配置其虚拟网络的防火墙网关和高级安全服务等策略，配置租户空间的虚拟网络、虚拟主机和访客虚拟机等云服务所必需的安全配置和管理任务（包括更新和安装补丁、容器安全管理、大数据分析等平台服务的租户配置以及其他各项租户租用的云服务内部的安全配置等）。							

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
DS-1.2	防火墙 / 广域网 / 周边安全	Deny all incoming and outgoing network requests by default. Enable only explicitly defined incoming requests by specific protocol and destination. Enable only explicitly defined outgoing requests by specific protocol and source.	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：在每个云数据中心边界部署华为专业的Anti-DDoS设备来完成对异常和超大流量攻击的检测及清洗。• 网络入侵检测与拦截：IPS具备网络实时流量分析和阻断能力，能防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。基于网络流量，IPS可以提供信息帮助定位和调查网络异常，分配定向流量的限制策略，并采用相应的自定义检测规则，保障生产环境内的应用程序和网络基础设施安全。• Web安全防护：华为云部署了Web应用防火墙应对Web攻击，如Web应用层的DDoS攻击、SQL注入、跨站脚本攻击、跨站请求伪造、组件漏洞攻击、身份伪造等。							
DS-1.2.1	防火墙 / 广域网 / 周边安全	Firewalls should be configured to actively alert security members of key security events	华为云内部制定防火墙管理规定，提出防火墙的对接设计要求及配置规范，并在安全事件响应流程中设置防火墙主备负责人。							

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
DS-1.3	防火墙 / 广域网 / 周边安全	Place externally accessible servers (e.g., web servers) within the DMZ.	华为云DMZ区主要部署了面向外网和租户的前置部件如负载均衡器、代理服务器等，以及服务部件如服务控制台、API 网关等。租户对DMZ区的访问行为不可信，所以需要对DMZ区单独隔离，防止外部请求接触云服务后端部件。此区域部件面临极高安全风险，除部署了防火墙、防DDoS 措施外，还部署了应用防火墙（ WAF ）及入侵检测与拦截设备IDS/IPS 以保护基础网路 、平台及应用。							
DS-1.4	防火墙 / 广域网 / 周边安全	Implement a process to patch network infrastructure devices (e.g., firewalls, routers, switches, etc.), SAN/NAS (Storage Area Networks and Network Attached Storage), and servers.	华为安全事件响应团队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。							

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
DS-1.5	防火墙 / 广域网 / 周边安全	Harden network infrastructure devices, SAN/NAS, and servers based on security configuration standards. Disable SNMP (Simple Network Management Protocol) if it is not in use or use only SNMPv3 or higher and select SNMP community strings that are strong passwords.	华为云建立了网络基础设施配置标准，网络基础设施的配置须按照标准执行，在标准中规范化各网络设备的接口、VLAN、SNMP等配置。							

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
DS-1.6	防火墙 / 广域网 / 周边安全	Do not allow direct management of the firewall from any external interfaces (i.e. Internet or WAN facing).	华为云对接入主机操作系统的华为云管理员执行严格的权限访问控制，对其所执行的各项运维运营操作实行全面的日志审计。 华为云管理员必须经过双因子认证后，才能通过堡垒机接入管理平面，所有操作都会记录日志并及时传送到集中日志审计系统。							

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
DS-1.7	防火墙 / 广域网 / 周边安全	Store local backups of network infrastructure/ SAN/NAS devices and servers on a server in a secure internal network.	《华为云用户协议》以及《隐私政策声明》中告知客户其个人数据的保留策略，华为云具有实现上述协议中的保留策略的技术能力。 除IAM/目标存储服务OBS以外，华为云上线的所有管理服务和组件的管理数据（包含操作日志等）均会备份到OBS中，而同时IAM/OBS的管理数据需要备份到非OBS存储。 客户可使用华为云提供的云备份CBR服务对云内的服务器、云硬盘、虚拟化环境提供备份服务。 客户可使用华为云云监控服务CES对服务器的运行状态、云上资源进行实时监控，当出现硬件故障时，云监控将会通过邮件、短信、HTTP/S通知客户。同时，客户可通过云硬盘EVS中的快照功能，当数据丢失时，可通过快照将数据完整的恢复到快照时间点。 华为云为客户提供镜像服务IMS产品，客户可通过该产品对云服务器的实例进行备份，当该实例的软件环境出现故障时，可以使用备份的镜像进行恢复。							

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
DS-1.8	防火墙 / 广域网 / 周边安全	Perform on at least a monthly basis network vulnerability scans of all external IP ranges and hosts and remediate issues. If applicable, the scope of external scans should include any cloud deployments.	华为云定期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，并聘请外部第三方对华为云的应用、网络进行渗透测试。 对于所有获知的安全漏洞信息，华为云将对每个漏洞进行评估分析，制定并落实漏洞修复方案或规避措施，并在修复后对修复情况进行验证，持续跟踪确认风险得到消除或缓解。							
DS-1.9	防火墙 / 广域网 / 周边安全	Perform on at least an annual basis, penetration testing of all external IP ranges and hosts and remediate issues.	华为云定期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及应用进行渗透测试，并对渗透测试的结果进行跟进与整改。							

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
DS-1.10	防火墙 / 广域网 / 周边安全	Secure any point to point connections by using dedicated, private connections and / or encryption.	对于华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，可以通过虚拟专用网络（VPN）、应用层TSL以及证书管理的方式保护任何点对点之间的连接。 客户可使用华为云数据加密服务DEW对传输的数据进行专属加密。 关于VPN、应用层TSL和证书管理、DEW更多的信息，可查阅《华为云安全白皮书》。							
DS-1.11	防火墙 / 广域网 / 周边安全	Implement a synchronized time service protocol (e.g., Network Time Protocol) 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
DS-1.12	防火墙 / 广域网 / 周边安全	Establish, document and implement baseline security requirements for WAN network infrastructure devices and services.	华为云基于严进宽用的原则，保障开源及第三方软件的安全引入和使用。 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。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。 同时，华为云要求服务发布前均需通过基本安全要求的验证，以保障基础架构的合规性。							

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
DS-2.0	互联网	Prohibit production network and all systems that process or store digital content from directly accessing the internet, including email. If a business case requires internet access from the production network or from systems that process or store digital content, only approved methods are allowed via use of a remote hosted application /	华为云边界保护设备配置为拒绝所有模式。使用规则集、访问控制列表（ACL）和配置的边界保护设备强制网络结构之间的信息流。这些设备以拒绝所有模式配置，需要设置经批准的防火墙以允许连接。	12.1 13			SOC1 3.1 SOC1 3.4 SOC1 3.14	IVS-08 IAM-05	1.1 1.2 1.3 1.4 2.2 5.1 6.6 8.5 11.2	CA-3 PL-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
		desktop session.								
DS-2.1	互联网	Implement email filtering software or appliances that block the following from non-production networks: • Potential phishing emails • Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.) • File size restrictions limited to 30 MB • Known domains that are sources of malware or viruses	华为云在网络边界部署DoS/DDoS防范清洗层、下代防火墙、入侵防御系统层以及网站应用防火墙层，保护华为云的互联网边界。 华为云限制接收和发送邮件的大小，对员工进行高频率的钓鱼邮件防范意识培训。							

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
DS-2.2	互联网	Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites.	华为云部署了 Web 应用防火墙应对 Web 攻击，如 Web 应用层的 DDoS 攻击、SQL 注入、跨站脚本攻击（XSS - Cross-Site Scripting）、跨站请求伪造（CSRF – Cross-Site Request Forgery）、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。							
DS-3.0	局域网 / 内部网络	Isolate the content/ production network from non-production networks (e.g., office network, DMZ, the internet etc.) by means of physical or logical network segmentation.	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（即内容/生产网络）、运维管理区。从外网访问数据存储区时，必须通过 DMZ 的服务控制台或网关才能访问。	6.2 9 10.1 11.2 12.3 12.6 13 16.1 17.1	12.3.1 12.6.1 13.1.3			IVS-06 IVS-07 IVS-08 IVS-11 IVS-12 IVS-13 TVM-02		AC-18 SI-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
DS-3.1	局域网 / 内部网络	Restrict access to the content / production systems to authorized computing hardware.	华为云对接入主机操作系统的华为云管理员执行严格的权限访问控制，对其所执行的各项运维运营操作实行全面的日志审计。 华为云管理员必须经过双因子认证后，才能通过堡垒机接入管理平面所有操作都会记录日志并及时传送到集中日志审计系统。					BCR-11 IAM-02		
DS-3.2	局域网 / 内部网络	Restrict remote access to the content / production network to only approved personnel who require access to perform their job responsibilities.	华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。员工的登陆、操作等日志将留存需要的时间以响应审核需求。							

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
DS-3.3	局域网 / 内部网络	Use switches/ layer 3 devices to manage network traffic. Disable all unused switch ports on the content / production network to prevent access from unauthorized devices.	华为云要求关闭所有未使用的端口，需要启用时再把端口打开。							
DS-3.4	局域网 / 内部网络	Restrict the use of non-switched devices such as hubs and repeaters on the content/ production network.	在内容/生产网络上，华为云均使用交换器，未使用集线器和中继器。							

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
DS-3.5	局域网 / 内部网络	Prohibit bridging or dual-homed networking (physical network bridging) on computer systems between content / production networks and non-content/ production networks.	华为云要求，未经批准，禁止将计算机同时接入两个或两个以上不同属性的网络。							
DS-3.6	局域网 / 内部网络	Implement a network-based intrusion detection / prevention system to protect the content / production network.	为了感知来自互联网以及租户虚拟网络之间东西向的攻击，并针对攻击实施阻断，华为云在网络边界部署了 IPS 设备，包括但不限于外网边界，安全区域边界和租户空间边界等。IPS 具备网络实时流量分析和阻断能力，能防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。基于网络流量，IPS 可以提供信息帮助定位和调查网络异常，分配定向流量的限制策略，并采用相应的自定义检测规则，保障生产环境内的应用程序和网络基础设施安全。							

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
DS-3.7	局域网 / 内部网络	Disable SNMP (Simple Network Management Protocol) if it is not in use. Use SNMPv3 or higher with strong passwords for community strings.	华为云使用安全的SNMP协议来保障公有云网络的安全。							
DS-3.8	局域网 / 内部网络	Harden systems prior to placing them in the LAN / Internal Network.	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（即内容/生产网络）、运维管理区，详情可见《华为云安全白皮书》。							
DS-3.9	局域网 / 内部网络	Conduct internal network vulnerability scans and remediate any issues, at least annually.	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。 对于所有获知的安全漏洞信息，华为云将对每个漏洞进行评估分析，制定并落实漏洞修复方案或规避措施，并在修复后对修复情况进行验证，持续跟踪确认风险得到消除或缓解。							

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
DS-3.10	局域网/内部网络	Store local backups of local area network, SAN/NAS, devices, servers and workstations on a server in a secure internal network.	除IAM/目标存储服务OBS以外，华为云上线的所有管理服务和组件的管理数据（包含操作日志等）均会备份到OBS中，而同时IAM/OBS的管理数据需要备份到非OBS存储。 客户可使用华为云提供的云备份CBR服务对云内的服务器、云硬盘、虚拟化环境提供备份服务。 客户负责对其内容数据进行加密存储。华为云的数据加密服务DEW可为客户提供在云硬盘EVS、对象存储OBS、云硬盘备份VBS等服务的加密存储功能。							
DS-3.11	局域网/内部网络	DNS servers used in the production network should not allow connections to and from the Internet.	DNS服务器部署在公共服务区，此区域内的部件根据业务需要受限开放给租户，且租户访问此区域部件和服务必须经过 DMZ 区。华为云管理员可以从内网区访问该区域进行操作和管理。 更多详细信息参考《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
DS-4.0	无线网络	Prohibit wireless networking and the use of wireless devices on the content / production network.	华为云禁止在内容/生产网络上使用无线网络和使用无线设备。	9.1 13.1				IVS-06 IVS-08 IVS-13 EKM-03	11.1	AC-18 SI-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
DS-4.1	无线网络	Configure non-production wireless networks (e.g., administrative and guest) with the following security controls: • Disable WEP / WPA • Enable WPA2-PSK (AES) • Segregate “guest” networks from the company’s other networks • Change default administrator logon credentials • Change default network name (SSID)	华为云内部办公网络的办公计算机均必须安装符合公司统一要求的安全软件，对员工、来宾网络进行分离，登录员工网络需要对员工身份进行验证。							

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
DS-4.2	无线网络	Implement a process to scan for rogue wireless access points and remediate any validated issues.	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。							
DS-5.0	I/O 设备安全	Designate specific data I/O systems to be used for uploading / downloading content from/ to external networks (Internet).	华为云对数据中心进出有严格的控制，未经允许，无法带入内容输入/输出设备。 管理人员管理服务器必须通过堡垒机，所有的输入输出被监控。 另外，虚拟化平台控制只有一个虚拟机的一个虚拟磁盘设备跟一个镜像文件关联。实现了虚拟机使用的虚拟设备与虚拟化。	10.7.1			SOC12.1 SOC15.1	IVS-08 IVS-09	7.1 8.2	SC-7 AC-19 MP-2

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
DS-5.0.1	I/O 设备安全	Implement a multi-layered network architecture for ingesting content from external networks (Internet) into the production network, and moving content from the production network to external networks.	华为云参考ITU E.408安全区域的划分原则并结合业界网络安全的优秀实践，对华为云网络进行安全区域、业务层面的划分和隔离。安全区域内部的节点具有相同的安全等级。 华为云从网络架构设计、设备选型配置到运行维护诸方面综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离接入控制和边界防护技术同时严格执行相应的管控措施确保华为云安全，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
DS-5.1	I/O 设备安全	Block input/output (I/O), mass storage, external storage, and mobile storage devices (e.g., USB, FireWire, Thunderbolt, SATA, Bluetooth, SCSI, etc.) and optical media burners (e.g., DVD, Blu-Ray, CD, etc.) on all systems that handle or store content, with the exception of systems used for content I/O. Refer to DS-4.0 for disconnecting	华为云对数据中心进出有严格的控制，未经允许，无法带入内容输入/输出设备。 管理人员管理服务器必须通过堡垒机，所有的输入输出被监控。 另外，虚拟化平台控制只有一个虚拟机的一个虚拟磁盘设备跟一个镜像文件关联。实现了虚拟机使用的虚拟设备与虚拟化。							

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
		wireless NICs.								
DS-6.0	系统安全	Install anti-virus and anti-malware software on all workstations, servers, and on any device that connects to SAN/NAS systems.	华为云使用IPS入侵防御系统、Web应用防火墙、防病毒软件以及HIDS主机型入侵检测系统对系统组件及网络进行漏洞管理。IPS入侵防御系统可以检测并预防潜在的网络入侵活动；Web应用防火墙部署在网络边界以保护应用软件的安全，使其免于受到来自外部的SQL注入、CSS、CSRF等面向应用软件的攻击；防病毒软件提供病毒防护及Windows系统内的防火墙；HIDS主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能。	6.2 8.1 9.4 10.1 11.1 11.2 12.1 12.2 12.5 12.6 14.1 14.2	9.4.4 12.6.1 14.1.1	A10.5		IVS-01 IVS-06 IVS-07 IVS-13 BCR-04 BCR-11 TVM-02 IAM-02 MOS-18 EKM-03 CCC-04		SI-3 SI-2 RA-5 AC-5 SC-2 PE-3 PE-5 MA-4 CM-10 CM-11 SI-7 AC-6 CM-7 CM-8
DS-6.1	系统安全	Update all anti-virus and anti-malware definitions daily, or more frequently.	华为云的防病毒软件会定期更新对防病毒和反恶意软件的策略库。							

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
DS-6.2	系统安全	Scan all content for viruses and malware prior to ingest onto the content / production network.	所有华为云产品与服务软件包发布上线前需对服务发布包（含补丁包）进行病毒扫描、数字签名、验证插件。					GRM-01 DCS-01		
DS-6.2.1	系统安全	Local firewalls should be implemented on workstations to restrict unauthorized access to the workstation.	华为云对员工按工作需要的最小范围分配权限，员工登录工作站需使用个人账户口令，并对其信息安全管理系统、敏感信息的访问、修改等操作进行监控和记录。							

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
DS-6.3	系统安全	Perform scans as follows: • Enable regular full system virus and malware scans on all workstations • Enable full system virus and malware scans for servers and for systems connecting to a SAN/NAS	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。							

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
DS-6.4	系统安全	Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patches/ updates that remediate security vulnerabilities.	与PCI DSS标准的相关要求保持一致，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。 对于所有获知的安全漏洞信息，华为云将对每个漏洞进行评估分析，制定并落实漏洞修复方案或规避措施，并在修复后对修复情况进行验证，持续跟踪确认风险得到消除或缓解。。							

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
DS-6.5	系统安全	Prohibit users from being Administrators on their own workstations, unless required for software (e.g., ProTools, Clipster and authoring software such as Blu-Print, Scenarist and Toshiba). Documentation from the software provider must explicitly state that administrative rights are required.	华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。当员工在岗状态发生变化时，及时对其权限进行清理与修改。 对接入主机操作系统的华为云管理员执行严格的权限访问控制，对其所执行的各项运维运营操作实行全面的日志审计。 华为云管理员必须经过双因子认证后，才能通过堡垒机接入管理平面，所有操作都会记录日志并及时传送到集中日志审计系统。							

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
DS-6.6	系统安全	Use cable locks on transportable computing devices that handle content (e.g., laptops, tablets, desktops, towers) when they are left unattended.	华为云内部制定了安全管理规定，对便携式计算设备进行严格管控，为控制信息流出，华为云不对机要岗位分配便携式计算机。							
DS-6.6.1	系统安全	Apply seals or tamper evident stickers on cases used for all workstations and servers that receive, send, manipulate, or store content in the production network.	华为云内部制定了安全管理规定，计算机的外设、USB等均已关闭，未经批准不得开通，计算机进入受控区域须进行安全配置。							

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
DS-6.7	系统安全	Implement additional security controls for laptops and portable computing storage devices that contain content or sensitive information relating to client projects. Encrypt all laptops. Use hardware-encrypted portable computing storage devices. Install remote-kill software on all laptops/ mobile devices that handle content to allow remote	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。客户负责对其内容数据进行加密存储。 华为云要求对于承载大量关键信息的便携机通过安装全盘加密等软件等措施防止设备丢失后数据泄密的风险。							

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
		wiping of hard drives and other storage devices.								
DS-6.8	系统安全	Restrict software installation privileges to IT management.	华为云所有的办公计算机均需安全公司指定的安全软件对计算机进行监控，并仅可以安装公司规定的安全软件列表中的软件。 华为云办公计算机上仅可安装限定的标准软件，不允许安装可超越系统、对象、网络、虚拟机和应用控制措施的程序，并对软件的安装进行监控。							
DS-6.9	系统安全	Implement security baselines and standards to configure systems (e.g., laptops, workstations, servers, SAN/ NAS) that are set up internally.	华为云为内部系统建立了安全基线标准，在内部系统投入使用前均需要参照基线对内部系统标准化。							

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
DS-6.10	系统安全	Unnecessary services and applications should be uninstalled from content transfer servers.	华为云办公计算机上仅可安装限定的标准软件，不允许安装可超越系统、对象、网络、虚拟机和应用控制措施的程序，并对软件的安装进行监控。							
DS-6.11	系统安全	Maintain an inventory of systems and system components.	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。							
DS-6.12	系统安全	Document the network topology and update the diagram annually or when significant changes are made to the infrastructure.	华为云维护及更新自身的网络架构图，并由负责网络安全的团队对网络架构的合规性进行跟踪确认。							

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
DS-7.0	帐户管理	Establish and implement an account management process for administrator, user, and service accounts for all information systems and applications that handle content.	华为云建立账号权限管理流程，通过对系统账号/权限的整个生命周期以及授权过程的有效管理和监控，降低安全风险。	8.1 9 12.1 12.4 18.2	9.2.1 9.2.2 9.2.3	A.10.8 A.10.9 A.10.10	SOC1 2.1 SOC1 2.2 SOC1 2.3 SOC1 2.4	IAM-02 IAM-05 IVS-08 IAM-10 IAM-12 IVS-01	7.1 8.1 8.2 10.6	AC-2 AC-6 AU-2 AU-3 AU-6 AU-12 IA-4 PS-4 PS-5 PE-2
DS-7.1	帐户管理	Maintain traceable evidence of the account management activities (e.g., approval emails, change request forms).	华为云对开通的账号添加其权限对应的监控策略并保留监控记录，使得账号使用过程中，一旦发现账号或授权方面的异常即可自动报警。							

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
DS-7.2	帐户管理	Assign unique credentials on a need-to-know basis using the principles of least privilege.	华为云建立特权账号管理要规定，要求特权账号必须遵循工作相关、最小化授权、审批受控原则。							
DS-7.3	帐户管理	Rename the default administrator accounts and other default accounts and limit the use of these accounts to special situations that require these credentials (e.g., operating system updates, patch installations, software updates).	华为云建立特权账号基线，对特权账号的创建、使用及回收进行统一管理，特权账号在所有物理设备、网络设备、操作系统、数据库的操作都会受到严格管控。							

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
DS-7.4	帐户管理	Segregate duties to ensure that individuals responsible for assigning access to information systems are not themselves end users of those systems (i.e., personnel should not be able to assign access to themselves).	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。							
DS-7.5	帐户管理	Monitor and audit administrator and service account activities.	华为云使用日志系统对管理员级别的访问进行监控，控制非管理员员工不具备超过其应有权限，如特权访问的权限。							

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
DS-7.6	帐户管理	Implement a process to review user access for all information systems that handle content and remove any user accounts that no longer require access quarterly.	与ISO27001标准的相关要求保持一致，华为云依据员工工作需要为其提供所需的最小权限，并定期对权限进行审阅，使系统用户及管理员的始终遵循最小权限原则。							
DS-7.7	帐户管理	Restrict user access to content on a per-project basis.	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。							

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
DS-7.8	帐户管理	Disable or remove local accounts on systems that handle content where technically feasible.	华为云本地账号由堡垒机进行管理，员工登录系统时会有堡垒机监控操作行为。							
DS-8.0	身份验证	Enforce the use of unique usernames and passwords to access information systems.	华为云为每一位员工提供了唯一的身份标识并根据工作职责划分权限，员工在每一次登陆对其身份进行验证，出现事故时可及时追溯日志进行问责。华为云IAM可帮助客户实现AAA规则，支持云平台的身份验证、授权以及问责机制。	9 10.1	9.2.4	A.10.8	SOC1 2.5	IAM-02 IAM-12 MOS-14 MOS-16	10.1 10.2 10.3	SI-4 AU-1 AU-2 AU-3 AU-6 AU-9 AU-11
DS-8.1	身份验证	Enforce a strong password policy for gaining access to information systems. Password policy should include guidance for service accounts.	系统为管理员和最终用户提供唯一的身份标识。同时将身份标识与所有可审计事件相关联。每次请求访问虚拟桌面前，系统会进行用户身份鉴别，身份鉴别机制使用的口令须达到一定的复杂度要求，例如长度要求、数字字母及特殊字符组合要求等。							

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
DS-8.2	身份验证	Consider the use of a Privileged Account Management (PAM) tool.	为维护平台安全，华为云对主机操作系统进行最小化裁剪并对服务做安全加固。同时，对接入主机操作系统的华为云管理员执行严格的权限访问控制 (PAM Privilege Access Management)，对其所执行的各项运维运营操作实行全面的日志审计。华为云管理员必须经过双因子认证后，才能通过堡垒机接入管理平面所有操作都会记录日志并及时传送到集中日志审计系统。							
DS-8.2.1	身份验证	Implement two-factor authentication (e.g., username / password and hard token / verification code text message) for access to web based e-mail (Google, Microsoft, etc.) from desktops or mobile computing devices.	华为云的IAM服务支持使用多因素认证用于登录验证和操作保护。开启了登录验证功能后，用户登录控制台时，除了需要输入用户名和密码外，还需要在登录验证页面输入验证码；开启了操作保护后，用户进行敏感操作时，需要输入验证码确认操作。多因素认证设备支持手机、邮箱和虚拟MFA设备。							

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
DS-8.3	身份验证	Implement password-protected screensavers or screen-lock software for servers and workstations.	依据SOC、PCI DSS和ISO27001等标准的要求，华为云建立对于员工的职责与应为规范进行规定，第三方审核机构会对华为云是否对所有计算机和笔记本电脑进行配置，以确保在预定义的时间之后锁定屏幕进行审查。							

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
DS-8.4	身份验证	Considering implementing additional authentication mechanisms to provide a layered authentication strategy for WAN and LAN / Internal Network access.	华为云的IAM服务支持使用多因素认证用于登录验证和操作保护。开启了登录验证功能后，用户登录控制台时，除了需要输入用户名和密码外，还需要在登录验证页面输入验证码；开启了操作保护后，用户进行敏感操作时，需要输入验证码确认操作。多因素认证设备支持手机、邮箱和虚拟MFA设备。 华为云支持基于SAML2.0协议的单点登录，客户可以使用华为云的身份提供商功能，实现用户使用企业身份提供商账号单点登录华为云。 目前华为云支持两种形式的联邦身份认证： • 浏览器页面单点登录（WebSSO）：浏览器作为通讯媒介，适用于普通用户通过浏览器访问华为云。 • 调用API接口：开发工具/应用程序作为通讯媒介，例如OpenStackClient、ShibbolethECPClient，适用企业或用户通过API调用方式访问华为云。							

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
DS-9.0	记录与监控	Implement real-time logging and reporting systems to record and report security events; gather the following information at a minimum: • When (time stamp) • Where (source) • Who (user name) • What (content)	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 。	10.1 12.4	12.4.1 12.4.3			IVS-02 EKM-02 IVS-06 IVS-13 SEF-05 SEF-02 IAM-02	10.1 10.2 10.3	AU-1 AU-2 AU-3 AU-6 AU-8 AU-9 AU-11 SI-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
DS-9.01	记录与监控	Implement logging mechanisms on all systems used for the following: • Key generation • Key management • Vendor certificate management	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。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CMK的操作活动等。							
DS-9.1	记录与监控	Implement a server to manage the logs in a central repository (e.g., syslog/log management server, Security Information and Event Management (SIEM) tool).	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。 华为云对提供的服务的网络设备、应用系统启用安全日志，日志对设备、系统的所有更改都会进行记录。							

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
DS-9.2	记录与监控	Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents.	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。 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。							
DS-9.3	记录与监控	Investigate any unusual activity reported by the logging and reporting systems.	华为云发布了《华为云安全白皮书》，其中介绍华为云主要负责安全事件的响应，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。华为云秉承快速发现、快速定界、快速隔离与快速恢复的安全事件响应原则。同时，根据安全事件对整网、客户的危害刷新事件定级标准以及响应时限和解决时限等要求。							

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
DS-9.4	记录与监控	Review all logs weekly, and review all critical and high daily.	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。 华为云对提供的服务的网络设备、应用系统启用安全日志，对设备、系统的所有更改都会进行记录。 同时，华为云有专门的内审部门，定期对运维流程各项活动日志进行审计。							

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
DS-9.5	记录与监控	Enable logging of internal and external content movement and transfers and include the following information at a minimum: • Username • Timestamp • File name • Source IP address • Destination IP address • Event (e.g., download, view)	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。							
DS-9.6	记录与监控	Retain logs for at least one year.	华为云日志大数据分析系统有强大的数据保存及查询能力，要求所有日志保存时间足够长，以支持特定的内审部门定期对运维流程各项活动进行审计。							

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
DS-9.7	记录与监控	Restrict log access to appropriate personnel.	华为云依照权限最小化原则分配员工的访问权限，员工仅可访问已授权的内容。对于日志的访问和审核权限只限于特定员工，其权限的审批需收到上级管理人员的批准，并定期进行审核。 华为云为客户提供云审计服务，客户可使用云日志服务对虚拟机的配置、日志的更改进行记录，使用云审计服务对于配置的日志的完整性进行监控。							
DS-10.0	移动安全	Define security controls and standards for mobile computing devices. *Refer to MS-4.0.2 for mobile computing device policies.*	华为云制定移动安全管理规定，以实施对移动计算设备的统一管理。	6.2 11.2				MOS-02 MOS-04 MOS-08 MOS-9 MOS-10 MOS-11 MOS-12		SCA IA-2

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
DS-10.1	移动安全	Develop a list of approved applications, application stores, and application plugins/ extensions for mobile devices accessing or storing content.	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，华为云为此建立并执行了相应的规章制度。 客户保留对其数据和相关媒体资产的控制和责任，有责任管理移动安全设备以及对客户内容的访问。					MOS-14 MOS-16 MOS-17 MOS-18 MOS-19		
DS-10.2	移动安全	Maintain an inventory of all mobile devices that access or store content.	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，华为云为此建立并执行了相应的规章制度。 客户保留对其数据和相关媒体资产的控制和责任，有责任管理移动安全设备以及对客户内容的访问。							

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
DS-10.3	移动安全	Require encryption either for the entire device or for areas of the device where content will be handled or stored.	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，华为云为此建立并执行了相应的规章制度。 客户保留对其数据和相关媒体资产的控制和责任，有责任管理移动安全设备以及对客户内容的访问。							
DS-10.4	移动安全	Prevent the circumvention of security controls.	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，华为云为此建立并执行了相应的规章制度。 客户保留对其数据和相关媒体资产的控制和责任，有责任管理移动安全设备以及对客户内容的访问。							
DS-10.5	移动安全	Implement a system to perform a remote wipe of a mobile device, should it be lost/ stolen/ compromised or otherwise necessary.	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，华为云为此建立并执行了相应的规章制度。 客户保留对其数据和相关媒体资产的控制和责任，有责任管理移动安全设备以及对客户内容的访问。							

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
DS-10.6	移动安全	Implement automatic locking of the device after 10 minutes of non-use.	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，华为云为此建立并执行了相应的规章制度。 客户保留对其数据和相关媒体资产的控制和责任，有责任管理移动安全设备以及对客户内容的访问。							
DS-10.7	移动安全	Manage all mobile device operating system patches and application updates.	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，华为云为此建立并执行了相应的规章制度。 客户保留对其数据和相关媒体资产的控制和责任，有责任管理移动安全设备以及对客户内容的访问。							
DS-10.8	移动安全	Enforce password policies.	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，华为云为此建立并执行了相应的规章制度。 客户保留对其数据和相关媒体资产的控制和责任，有责任管理移动安全设备以及对客户内容的访问。							

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
DS-10.9	移动安全	Consider implementing a system to perform backup and restoration of mobile devices.	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，华为云为此建立并执行了相应的规章制度。 客户保留对其数据和相关媒体资产的控制和责任，有责任管理移动安全设备以及对客户内容的访问。							
DS-11.0	安全技术	Ensure that security techniques (e.g., spoiling, invisible/visible watermarking) are available for use and are applied when instructed.	当需要对数据进行版权保护、真伪鉴别、流转跟踪时，客户可以选择数字水印技术。华为云的对象存储服务具备对图片添加文字或图片类型水印的功能，支持通过控制台图形界面、代码编辑模式和接口调用多种使用模式便利客户对图片进行水印设置，并快速获取到处理后的图片。	8.2.10.1	12.3.1		SOC1 4.3 SOC1 4.4 SOC1 4.5 SOC1 4.6 SOC1 4.7 SOC1 4.8	EKM-01 EKM-03 EKM-04 HRS-05	3.4 3.5 3.6 4.1	IA-5 SC-8 SC-9 SC-12 SC-13

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
DS-11.1	安全技术	Encrypt content on hard drives or encrypt entire hard drives using a minimum of AES-256 encryption by either: • File-based encryption: (i.e., encrypting the content itself) • Drive-based encryption: (i.e., encrypting the hard drive)	华为云使用数据快递服务(DES)解决海量数据传输的难题，如高昂的网络成本、较长传输时间等。DES支持第三方加密工具使用业界通用的AES256加密算法对数据进行客户端加密。工具不需要生成任何文件即可在硬盘上建立虚拟磁盘 。 用户可以按照盘符进行访问，所有虚拟磁盘上的文件都被自动加密，必须使用密码来进行访问。							

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
DS-11.2	安全技术	Send decryption keys, keypad pins, or passwords using an out-of-band communication protocol (i.e., not on the same storage media as the content itself).	华为云自身使用行业广泛使用的AES强效加密法对平台内数据进行加密，在传输过程中使用高版本TLS加密协议保障数据安全。 客户可使用数据加密服务对数据进行加密，华为云提供不同厂商、不同规格（标准加密算法、国密算法等）、不同强度的云HSM供租户选择，满足不同租户的实际需求。							

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
DS-11.3	安全技术	Implement and document key management policies and procedures: • Use of encryption protocols for the protection of sensitive content or data, regardless of its location (e.g., servers, databases, workstations, laptops, mobile devices, data in transit, email) • Approval and revocation of trusted devices • Generation,	根据华为云密钥管理策略，每个用户具有唯一的ID标识其身份。 客户可以使用IAM的密钥管理服务KMS为可识别的所有者绑定密钥。 华为云推出的数据加密服务DEW，支持密钥托管，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，并记录密钥的所有权。							

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
		renewal, and revocation of content keys • Internal and external distribution of content keys • Bind encryption keys to identifiable owners • Segregate duties to separate key management from key usage • Key storage procedures • Key backup procedures								

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
DS-11.4	安全技术	Encrypt content using a minimum of AES-256 encryption.	华为云自身使用行业广泛使用的AES强效加密法对平台内数据进行加密，在传输过程中使用高版本TLS加密协议保障数据安全。 客户可使用数据加密服务对数据进行加密，华为云提供不同厂商、不同规格（标准加密算法、国密算法等）、不同强度的云HSM供租户选择，满足不同租户的实际需求。							

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
DS-11.5	安全技术	Store secret and private keys (not public keys) used to encrypt data/ content in one or more of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (e.g., Host Security Module (HSM) or	通过密钥管理服务KMS用户能够方便地管理自己的密钥，并能随时使用数据加密密钥DEK进行数据加密，确保关键业务数据的安全。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。HSM采用双机部署，保证HSM的高可靠性和高可用性。CMK经过根密钥加密后，以密文的形式保存在密钥存储节点中。 另外，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。							

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
		a Pin Transaction Security (PTS) point-of-interaction device), having at least two full-length key components or key shares, in accordance with a security industry accepted method								

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
DS-11.6	安全技术	Confirm that devices on the Trusted Devices List (TDL) are appropriate based on rights owners' approval.	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。 华为云所有的办公计算机均需安全公司指定的安全软件，仅可以安装指定软件列表的软件。对于IT基础系统、组件则通过IDS/IPS等方式进行保护。安全软件、基础设施组件安装杀毒软件等安全软件，并限制安全软件的配置修改权限以及对其要求强制更新。华为云所有的办公计算机均需安全公司指定的安全软件，仅可以安装指定受信任软件列表的软件，不支持运行移动代码。							

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
DS-11.6.1	安全技术	Access to KDMs must be restricted to the KDM creator and exhibitor only.	华为云为客户提供数据加密服务DEW，它可以提供密钥管理（KMS）功能。 为保障客户密钥的安全可靠，KMS 基于 IAM 角色统一进行 RBAC 访问控制。对于用户，只有通过IAM 身份验证及 KMS 鉴权，并设置了密钥操作权限的用户，才能操作 KMS 中存储的主密钥（CMK）。仅设置了只读权限的用户只能查询 CMK 信息，不能对 CMK 进行操作。KMS 对 CMK 进行了客户隔离，每一个客户只能访问与管理属于自己的 CMK，无法操作其他客户的 CMK。此外，系统管理员仅有设备管理权限，没有任何访问 CMK 的权限。							
DS-11.6.2	安全技术	KDM creation and handling must be physically and digitally segregated from DCP handling and replication where feasible.	KMS 的根密钥保存在 HSM（硬件安全模块）中，从来不会出现在 HSM 之外，保证根密钥不泄露。 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。							

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
DS-11.7	安全技术	Confirm the validity of content keys and ensure that expiration dates conform to client instructions.	客户可使用华为云数据加密服务DEW进行专属加密、密钥管理及密钥对管理，支持密钥创建、授权、自动轮换以及密钥硬件保护。客户可根据需要自主选择其所需的密钥管理机制。							
DS-12.0	内容跟踪	Implement a digital content management system to provide detailed tracking of digital content.	华为云从数据访问控制、安全防护、审计等方面为客户提供了相关服务，协助客户对数据的使用和流转做到更加细粒度的管控，以避免信息泄露和法律法规遵从上带来的的风险。							

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
DS-12.1	内容跟踪	Retain digital content movement transaction logs for one year.	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。 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。 对于对象存储、文件存储等服务，客户可以使用云审计服务 (CTS) 来记录用户对数据的操作。							
DS-12.2	内容跟踪	Review logs from digital content management system periodically and investigate anomalies.	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。							

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
DS-12.3	内容跟踪	Use client AKAs（“aliases”）in asset tracking systems, unless otherwise as directed by the client.	根据ISO27001标准，华为云的信息资产分类由专门的工具进行监控和管理，形成资产清单，每个资产均有唯一的资产编号。 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。 华为云从数据访问控制、安全防护、审计等方面为客户提供了相关服务，协助客户对数据的使用和流转做到更加细粒度的管控，以避免信息泄露和法律法规遵从上带来的的风险。							

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
DS-12.4	内容跟踪	Use enterprise (not personal) versions of online or web based collaboration services (e.g., Google Docs, etc.) for tracking content, managing inventory, or workflow management, Utilize multi-factor authentication and centrally managed user accounts and access to data.	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。 华为云统一身份认证服务（IAM Identity and Access Management）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。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。							

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
DS-13.0	传输系统	Use only client-approved transfer systems that utilize access controls, a minimum of AES-256 encryption for content at rest and for content in motion and use strong authentication for content transfer sessions.	华为云自身使用行业广泛使用的AES强效加密法对平台内数据进行加密，在传输过程中使用高版本TLS加密协议保障数据安全。另外，IAM 通过提供基于 IP 的 ACL 可以限制企业用户只在安全的网络环境下访问华为云资源，避免企业用户因接入不安全网络环境导致的数据泄露。	10.1 13.2		A.10.6	SOC1 4.3 SOC1 4.4 SOC1 4.5 SOC1 4.6 SOC1 4.7 SOC1 4.8		3.4 3.5 3.6 4.1	IA-5 SC-13

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
DS-13.1	传输系统	Implement an exception process, where prior client approval must be obtained in writing, to address situations where encrypted transfer tools are not used.	华为云服务提供REST和Highway方式进行数据传输，两种数据传输方式均支持使用传输层安全协议TLS1.2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。							
DS-14.0	传输设备的使用方法	Implement and use dedicated systems for content transfers.	华为云提供服务支持第三方加密工具使用业界通用的AES 256 加密算法对数据进行客户端加密。 DES 支持的客户端是Windows 、 Mac OS X 、Linux等操作系统。	12.4 13.1 13.2		A.4.1				AC-4 AC-20 SC-7 MP-6
DS-14.1	传输设备的使用方法	Separate content transfer systems from administrative and production networks.	客户在开通数据传输服务后登录管理控制台创建服务单，将数据按要求加密存放入待邮寄磁盘中后，即可将磁盘邮寄快递至华为云数据中心。							

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
DS-14.2	传输设备的使用方法	Place content transfer systems in a Demilitarized Zone (DMZ) and not in the content / production network. Implement whitelisting on content transfer servers to only allow transfers to and from authorized external transfer servers.	华为云在DMZ区部署了了面向外网和租户的前置部件和服务部件，从外网访问时内容生产网络时，需要通过DMZ区的服务控制台或者网关。更多相关信息可以查看《华为云安全白皮书》。							
DS-14.3	传输设备的使用方法	Remove content from content transfer devices/ systems immediately after successful transmission/ receipt.	华为云在DMZ区部署了面向外网和租户的前置部件和服务部件，从外网访问时内容生产网络时，需要通过DMZ区的服务控制台或者网关。更多相关信息可以查看《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
DS-14.4	传输设备的使用方法	Send automatic notifications to the production coordinator(s) upon outbound content transmission.	华为云为客户提供云审计服务（CTS Cloud Trace Service ），CTS可以实时、系统地记录用户在管理界面上的所有操作和用户在华为云上的所有 API 操作，便于客户进行问题查询、分析与定位。							
DS-15.0	客户门户	Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users.	客户需承担其自身数据的访问控制责任，确保其访问权限有效设置以避免不当访问。 客户可参考华为云IAM产品文档中的最佳实践，制定自身的职责分离策略，以及如何安全使用IAM。	9.2 9.4 10.1 12.1 12.6 13.1 13.2		A.10.8				AC-2 AC-3 AC-4 AC-6 AC-20 IA-5 SC-3 SC-8 SI-7

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
DS-15.1	客户门户	Assign unique credentials (e.g., username and password) to portal users and distribute credentials to clients securely.	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》。客户需承担其自身数据的访问控制责任，确保其访问权限有效设置以避免不当访问。 客户可参考华为云IAM产品文档中的最佳实践，制定自身的职责分离策略，以及如何安全使用IAM。							
DS-15.2	客户门户	Ensure users only have access to their own digital assets (i.e., client A must not have access to client B’s content).	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。							
DS-15.3	客户门户	Place the web portal on a dedicated server in the DMZ and limit access to/ from specific IPs and protocols.	华为云对客户访问 DMZ 区进行限制， 对 DMZ 单独隔离，防止外部请求接触云服务后端部件 。							

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
DS-15.4	客户门户	Prohibit the use of third-party production software/ systems/ services that are hosted on an internet web server unless approved by client in advance.	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。							

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
DS-15.5	客户门户	Use HTTPS and enforce use of a strong cipher suite (e.g., TLS v1.3) for the internal/ external web portal. Acquire an HTTPS public key certificate signed by a certificate authority trusted by a majority of web browsers.	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》。 华为云为租户提供证书管理服务（SSL Certificate Service），联合全球知名数字认证机构，对X.509 证书进行一站式的全生命周期管理，实现目标网站的可信身份认证与安全数据传输。							

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
DS-15.6	客户门户	Do not use persistent cookies or cookies that store credentials in plaintext.	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。 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。							
DS-15.7	客户门户	Set access to content on internal or external portals to expire automatically at predefined intervals, where configurable.	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》。客户需承担其自身数据的访问控制责任，确保其访问权限有效设置以避免不当访问。 客户可参考华为云IAM产品文档中的最佳实践，制定自身的职责分离策略，以及如何安全使用IAM。							

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
DS-15.8	客户门户	Test for web application vulnerabilities quarterly and remediate any validated issues.	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。 华为云提供漏洞扫描服务（Vulnerability Scan Service），集Web漏洞扫描、资产内容合规检测、弱密码检测三大核心功能，自动发现网站或服务器在网络中的安全风险，为云上业务提供多维度的安全检测服务。							
DS-15.9	客户门户	Perform annual penetration testing of web applications and remediate any validated issues.	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。 华为云已与合作伙伴联合推出了主机入侵检测、 Web 应用防火墙、主机漏洞检测、网页防篡改服务及渗透测试等服务，提升了华为云的安全检测、感知及防御能力，详见《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
DS-15.10	客户门户	Allow only authorized personnel to request the establishment of a connection with the telecom service provider.	客户可参考华为云IAM产品文档中的最佳实践，制定自身的职责分离策略，以及如何安全使用IAM。 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》。客户需承担其自身数据的访问控制责任，确保其访问权限有效设置以避免不当访问。							
DS-15.11	客户门户	Prohibit transmission of content using email (including webmail).	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》。 客户可考虑使用安全的电子邮件设备服务器对电子邮件和附件进行加密，华为云提供数据加密服务（DEW），该服务提供专属加密、密钥管理、密钥对管理等功能。							

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
DS-15.12	客户门户	Review access to the client web portal at least quarterly.	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》。							

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
DS-15.13	客户门户	Implement a process to review the facility's public informational website and other online industry resources for sensitive information that could be leveraged by an attacker (e.g. mentions of internal infrastructure and technologies, content transfer servers, IP addresses, photos of sensitive areas, current content being worked on, etc.)	客户需承担其自身数据的访问控制责任，确保其访问权限有效设置以避免不当访问。 华为云为客户提供云监控服务、应用运维管理AOM、应用性能管理APM以帮助客户持续监控华为云提供的服务的各项指标，支持通过OpenAPI、SDK、Agent方式上报自定义指标，触发警告将及时通知客户。							

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1月	1.0	首次发布

