

华为云沙特阿拉伯网络安全遵从性指南

文档版本 1.1
发布日期 2023-12-25



版权所有 © 华为云计算技术有限公司 2023。保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

目 录

1 概述.....	1
1.1 背景与发布目的	1
1.2 适用的沙特阿拉伯的网络安全监管要求简介	1
1.3 名词定义	2
2 华为云安全合规.....	3
3 华为云安全责任共担	6
4 华为云全球基础设施	7
5 华为云如何符合《ECC 基本网络安全控制》的要求	8
5.1 网络安全治理	8
5.1.1 网络安全战略	8
5.1.2 网络安全管理	9
5.1.3 网络安全政策与程序	10
5.1.4 网络安全角色与责任	11
5.1.5 网络安全风险管理	11
5.1.6 信息技术项目管理中的网络安全	13
5.1.7 网络安全标准、法律及法规合规	15
5.1.8 定期网络安全审查与审计	16
5.1.9 人力资源网络安全	17
5.1.10 网络安全意识和培训计划	18
5.2 网络安全防御	20
5.2.1 资产管理	20
5.2.2 身份与访问管理	22
5.2.3 信息系统与信息处理设施保护	24
5.2.4 电子邮件保护	27
5.2.5 网络安全管理	28
5.2.6 移动设备安全	32
5.2.7 数据和信息保护	33
5.2.8 密码学	35
5.2.9 备份与恢复管理	38

5.2.10 漏洞管理	40
5.2.11 渗透测试	43
5.2.12 网络安全事件日志与监控管理.....	44
5.2.13 网络安全事件与威胁管理	47
5.2.14 物理安全	49
5.2.15 Web 应用安全	51
5.3 网络安全弹性	53
5.3.1 业务连续性管理 (BCM) 的网络安全弹性方面	53
5.4 第三方与云计算网络安全	56
5.4.1 第三方网络安全	56
5.4.2 云计算与托管网络安全	59
6 华为云如何符合《CCC 云计算控制》的要求.....	61
6.1 网络安全治理	61
6.1.1 网络安全角色与责任	61
6.1.2 网络安全风险管理	62
6.1.3 网络安全标准、法律和法规合规.....	62
6.1.4 人力资源网络安全	63
6.1.5 网络安全变更管理	64
6.2 网络安全防御	65
6.2.1 资产管理	65
6.2.2 身份与访问管理	66
6.2.3 信息系统和信息处理设施保护.....	68
6.2.4 网络安全管理	72
6.2.5 移动设备安全	74
6.2.6 数据和信息保护	75
6.2.7 密码学	76
6.2.8 备份与恢复管理	77
6.2.9 漏洞管理	78
6.2.10 渗透测试	78
6.2.11 网络安全事件日志与监控管理.....	79
6.2.12 网络安全事件与威胁管理	80
6.2.13 物理安全	82
6.2.14 Web 应用安全	82
6.2.15 密钥管理	83
6.2.16 系统开发安全	84
6.2.17 存储介质安全	86
6.3 网络安全弹性	87
6.3.1 业务连续性管理 (BCM) 的网络安全弹性	87
6.4 第三方网络安全	88

6.4.1 供应链与第三方网络安全	88
7 华为云如何符合《CRF 网络安全监督框架》的要求	90
7.1 网络安全治理	90
7.1.1 网络安全策略	90
7.1.2 网络安全管理	91
7.1.3 网络安全合规	93
7.1.4 网络安全审计	94
7.1.5 网络安全意识&培训	95
7.1.6 项目管理中的网络安全	97
7.1.7 人力资源中的网络安全	98
7.2 资产管理	101
7.2.1 资产发现	101
7.2.2 资产分类	103
7.2.3 自带设备	104
7.2.4 可接受的使用策略	105
7.2.5 资产维护	106
7.2.6 资产的安全处置	107
7.3 网络安全风险管理	108
7.3.1 网络安全风险评估	108
7.3.2 网络安全风险处置与监控	110
7.4 逻辑安全	111
7.4.1 密码学	111
7.4.2 变更管理	114
7.4.3 漏洞管理	115
7.4.4 补丁管理	117
7.4.5 网络安全	119
7.4.6 日志与监控	125
7.4.7 身份和访问管理和特权访问管理	129
7.4.8 应用程序白名单	133
7.4.9 事件管理	134
7.4.10 恶意软件处理	138
7.4.11 信息保护	141
7.4.12 备份与恢复管理	144
7.4.13 配置管理与加固	149
7.4.14 安全软件开发	151
7.4.15 电子邮件和网络浏览器保护	154
7.4.16 渗透测试	155
7.5 物理安全	156
7.5.1 安全设备和区域	156

7.5.2 物理访问管理	158
7.5.3 环境保护	160
7.5.4 场外资产	160
7.6 第三方安全	161
7.6.1 云服务	161
7.6.2 外包服务	163
8 结语	167
9 历史版本.....	168

1 概述

1.1 背景与发布目的

在科技发展的浪潮中，越来越多的组织在逐渐寻求业务转型并希望借助先进信息技术以降低成本、提升运营效率、实现业务模式的创新。不过，在信息技术得到广泛运用的同时，网络安全事件也随之不断出现。为了规范对信息技术的运用，巩固与提升国家网络安全水平，沙特阿拉伯国家网络安全局（NCA）与通信、空间和技术委员会（CST）发布了一系列网络安全监管要求。

华为云作为云服务供应商，致力于协助客户满足这些监管要求，持续为客户提供符合监管要求的云服务及业务运行环境。本文将针对客户在使用云服务时通常需遵循的沙特阿拉伯网络安全监管要求，详细阐述华为云将如何协助其满足这些监管要求。

1.2 适用的沙特阿拉伯的网络安全监管要求简介

国家网络安全局（NCA）：是主要负责沙特阿拉伯网络安全相关的监管和运营职能，负责该国网络安全的政府实体，它与公共和私营实体密切合作，以改善国家的网络安全态势，以维护其重要利益、国家安全、关键基础设施、高优先级部门和政府服务和符合 2030 年愿景的活动。

- **《ECC 基本网络安全控制》：**基本网络安全控制考虑了沙特阿拉伯王国所有组织和部门的网络安全需求，是关键国家基础设施（CNI）组织必须遵守最低网络安全要求。
- **《CCC 云计算控制》：**云计算控制是对基本网络安全控制的扩展和补充，旨在从云服务提供商和云服务租户的角度定义云计算的网络安全要求，以提高安全性并降低所有服务和用户的网络风险。

通信、空间和技术委员会（CST）：负责组织沙特阿拉伯王国的通信、空间和信息技术部门，监督制定 ICT 相关法规的标准化。该组织向运营商提供许可证，规范该行业，并监控国家境内互联网的使用。该组织前身是沙特通信和信息技术委员会（CITC）。2022 年 11 月 10 日，沙特通信和信息技术委员会（CITC）正式更名为沙特通信、空间和技术委员会（CST）。

- 《CRF 网络安全监督框架》：旨在提高信息和电信部门（ICT）的网络安全成熟度。CRF 要求按照国际最佳实践和当地网络安全法规来更好地管理网络安全风险，LSP 必须实施这些要求，以满足最低安全要求。

1.3 名词定义

- **华为云**

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

- **资产**

对组织有价值的任何有形或无形的东西。包含各种类型的资产，例如：人员、机器、公共事业、专利、软件、服务、信息和特征。

- **服务提供商**

根据外包安排向组织提供服务的实体以及实体的分支机构。

- **关键国家基础设施 (CNI)**

这些资产（即设施、系统、网络、流程以及操作和处理它们的关键运营商）的损失或易受安全漏洞影响可能导致：

- 对基本服务的可用性、整合或交付产生重大负面影响，包括可能导致严重财产损失和/或生命和/或伤害的服务，以及对经济和/或社会的重大影响。
- 对国家安全和/或国防和/或国家经济或国家能力产生重大影响。

- **云技术堆栈**

实现云计算服务必不可少的技术分层架构：（数据中心基础设施、局域网、存储/计算/超融合硬件、管理程序、云管理平台、虚拟设备、操作系统、应用软件、运维平台、云安全技术等）。

- **密码学原语**

一种用于为安全系统构建密码协议的低级算法。它被密码设计者用作他们最基本的构建块。这些构建块是密码系统的一部分，密码系统是实现特定安全服务所需的一套密码算法，例如加密函数或单向哈希函数。

- **LSP**

CST 许可或注册的组织。

2 华为云安全合规

华为云继承了华为公司完备的管理体系以及 IT 系统建设、运营经验，对云服务各项服务的集成、运营、维护进行主动管理，并持续改进。同时，华为云一如既往地确保其基础设施和云服务通过业界认可的独立第三方安全权威组织的测评以及安全认证机构的审核。截至目前为止，华为云已获得众多国际和行业安全合规资质认证，全力保障云服务客户所部署业务的安全与合规。

华为云服务和平台已获得以下认证：

认证	描述
ISO 27001:2013	ISO 27001 是一种被广泛使用的国际标准，它规定了信息安全管理体系建设的要求。基于定期风险评估，该标准提供了一套评估组织信息和客户信息管理体系的方法。
网络安全等级保护	网络安全等级保护是公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键 Region、节点通过了网络安全等级保护四级。
ISO 27017:2015	ISO 27017 是针对云计算信息安全的国际认证。ISO 27017 的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
新加坡 MTCS Level 3 认证	MTCS 多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求 CSP 在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得 MTCS 最高安全评级的 Level 3 等级认证。
ISO 20000-1:2011	ISO 20000 是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务提供商可提供有效的 IT 服务来满足客户和业务的需求。
SOC 审计	SOC 审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。
ISO 27018:2014	ISO 27018 是首个专注于云中个人数据保护的国际行为准则。

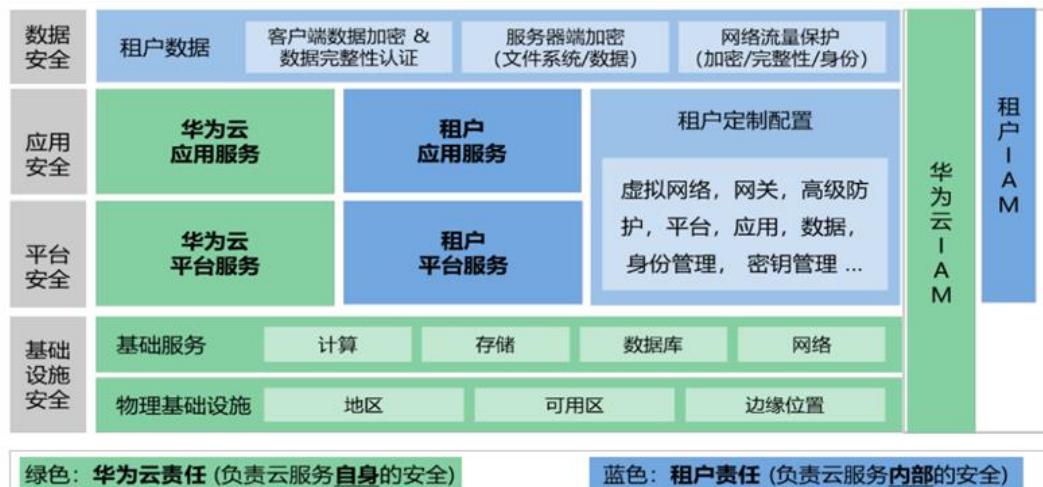
	则。ISO 27018 的通过，表明华为云已拥有完备的个人数据保护管理系统，在数据安全管理方面处于全球领先地位。
PCI DSS 认证	支付卡行业数据安全标准（PCI DSS）是由 JCB、美国运通、Discover、万事达和 Visa 等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。
ISO 22301:2012	ISO 22301 是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
CSA STAR 金牌认证	CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和 CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
TRUCS	可信云服务（TRUCS）是中国公共云领域最权威的认证之一。该认证表明，华为云符合中国最详细的云服务数据和服务保证认证标准。
可信云金牌运维专项评估	金牌运维评估是面向已通过可信云服务认证的云服务提供商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、健全的运维管理体系，符合国内权威云服务运营和维护保障要求的认证标准。
云服务用户数据保护能力认证	该认证是《网络安全法》生效后中国首个云服务用户数据安全评估机制。华为云第一批通过了这一认证。
工信部云计算服务能力评估	ITSS 云计算服务能力评估基于国家标准，如《信息技术云计算云服务运营通用要求》。这是中国第一个云服务/云计算领域的分级评估机制。华为私有云和公有云双双获得云计算服务能力“一级”合规证书，这使华为成为数不多的“双冠供应商”之一。
可信云评估	可信云评估是由数据中心联盟（DCA）组织、中国信息通信研究院（工信部电信研究院）测评的面向云计算服务和产品的权威评估。
网信办网络安全审查	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云政务服务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。
国际通用准则 CC EAL3+	CC (Common Criteria)认证是一种被高度认可的信息技术产品和系统安全的国际评估标准。华为云 FusionSphere 已经通过了 CC EAL 3+认证，表明华为云软件平台在全球得到

	高度认可。
--	-------

3 华为云安全责任共担

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

基于责任共担模型，华为云与租户主要承担如下责任：



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

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

关于华为云与租户的安全责任详情，可参考华为云已发布的《华为云安全白皮书》。

4 华为云全球基础设施

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

5 华为云如何符合《ECC 基本网络安全控制》的要求

《ECC 基本网络安全控制》为组织中的信息和技术资产设定最低的网络安全要求，为客户进行网络安全风险管理提供了通用原则和最佳实践，将帮助组织最大限度地减少来自内部和外部的网络安全风险威胁。其中涵盖了网络安全治理、网络安全防御、网络安全弹性、第三方与云计算网络安全及工业控制系统网络安全五大领域。

以下内容将总结 ECC 中与云服务供应商相关的控制要求，并详细阐述了华为云作为客户的云服务供应商时，会如何帮助客户满足这些控制要求。

5.1 网络安全治理

“网络安全治理”要求客户建立适当的网络安全管理机制，涵盖网络安全战略、意识与培训、策略与程序、角色与责任、风险管理等网络安全治理领域。相关控制要求及华为云的实践方式如下：

5.1.1 网络安全战略

网络安全战略的目标是确保网络安全计划、目标、倡议和项目有利于相关法律法规的合规。

编号	具体控制要求	华为云的内部实践	客户的职责
1-1-1	应定义、记录和批准网络安全战略。该战略应得到组织负责人或其代表（在本文件中称为授权官员）的支持。战略目标应符合相关法律法规。	华为云制定了网络安全与隐私保护的管理要求，其中明确了华为云将构筑并全面实施端到端的网络安全体系作为重要战略，遵从业务所在地适用的法律法规，全面满足客户的网络安全需求。该战略得到公司最高管理层的批准。	客户应定义其网络安全战略，战略目标应符合相关法律法规的规定，战略应得到组织负责人或代表的批准支持。
1-1-2	应执行路径图以实施网络安全战	华为云在公司战略的指导下制定中长期的发展规划，支撑华为云业务	客户应根据网络安全战略制定实

	略。	的持续发展，并制定年度业务计划及实施路径图，其中包含网络安全相关活动、适用的法律法规的合规要求、开展和建立各类网络安全项目等，确保网络安全战略的有效落实。	施路径图或实施计划，以确保网络安全战略的落实。
1-1-3	应根据计划的时间间隔或相关法律法规的变化定期审查网络安全策略。	华为云至少每年审查一次网络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。同时华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性，向最高管理层报告调查的结果和建议。	客户应根据计划的频率或外部监管的变化定期对网络安全策略进行审查和更新。

5.1.2 网络安全管理

根据相关法律法规，确保授权官员支持在组织内实施和管理网络安全计划。

编号	具体控制要求	华为云的内部实践	客户的职责
1-2-1	应在组织内建立专门的网络安全职能（例如，部门）。此职能必须独立于信息技术/信息通信和技术 (IT/ICT) 职能（根据 14/8/1438H 的第 37140 号皇家法令）。强烈建议此网络安全功能在确保不会导致利益冲突的同时直接向组织负责人或其代表报告。	在华为公司层面，全球网络安全与用户隐私保护团队 GSPC 作为最高网络安全管理机构，决策和批准公司总体网络安全战略。GSPO 及其办公室负责制定和执行华为端到端网络安全保障体系。华为云网络安全与用户隐私保护团队负责制定华为云安全策略，并定期对策略的执行情况进行定期审视，确保安全治理的策略、规范和具体措施在各业务领域的流程落地，实现端到端的安全治理。同时，华为云在各产品、服务的业务团队中明确规定了所有员工对应角色的网络安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的安全管理职责。网络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。	客户应在组织内建立专门的网络安全职能。此职能须独立于信息技术/信息通信和技术 (IT/ICT) 职能。此外该网络安全职能在确保不会导致利益冲突的同时可直接向组织负责人或其代表报告。
1-2-3	授权官员必须建立一个网络安全指导委员会，以确保在组织内支持和实施网络安全。	在华为公司层面，全球网络安全与用户隐私保护团队 GSPC 作为最高网络安全管理机构，决策和批准公司总体网络安全战略。全球网络安全与用户隐私保护官 GSPO 及其办	客户组织负责人或其代表必须建立一个网络安全指导委员会，支持和实施网络安全计划。

	全计划和倡议。应定义、记录和批准委员会成员、角色和职责以及治理框架。该委员会必须将网络安全职能负责人作为其成员之一。强烈建议委员会在确保不会导致利益冲突的同时直接向组织负责人或其代表报告。	公室负责制定和执行华为端到端网络安全保障体系。华为云网络安全与用户隐私保护团队负责制定华为云安全策略，并定期对策略的执行情况进行定期审视，确保安全治理的策略、规范和具体措施在各业务领域的流程落地，实现端到端的安全治理。沙特网络安全与隐私保护官遵循公司最高层面的网络安全战略，并在沙特执行落地。	同时应定义委员会成员、角色和职责以及治理框架。此外该委员会在确保不会导致利益冲突的同时可直接向组织负责人或其代表报告。
--	--	--	---

5.1.3 网络安全政策与程序

确保组织根据相关法律法规和组织要求记录、传达和遵守网络安全要求。

编号	具体控制要求	华为云的内部实践	客户的职责
1-3-1	网络安全政策和程序必须由网络安全部门定义和记录功能，经授权官员批准，并分发给内部和组织之外相关方。	华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。网络安全政策和程序发布前需得到管理者审批，员工可根据授权查看已发布的信息安全政策和程序。同时，华为云针对公司政策、文化等方面每年定期开展员工培训。	客户的网络安全部门应制定网络安全政策和程序，并获得组织负责人或代表的批准，分发给组织的内外部相关方。
1-3-2	网络安全职能部门必须确保网络安全政策与程序的实施。	秉承华为网络安全战略和规范，华为云网络安全与用户隐私保护团队负责制定华为云安全策略，并定期对策略的执行情况进行定期审视，确保安全治理的策略、规范和具体措施在各业务领域的流程落地，实现端到端的安全治理。	客户的网络安全职能部门须确保网络安全政策与程序的实施。
1-3-3	网络安全政策与程序应得到技术安全标准的支持（例如，操作系统、数据库和防火墙技术安全标准）。	华为云参照各类国际、行业标准，法律法规监管要求以及业内的最佳实践，包括但不限于 CIS、PCI DSS、NIST CSF、CSA CCM 等，并结合业务所在地的安全合规要求，建立了一套完善的网络安全政策与程序。	网络安全政策与程序可参考业内技术安全标准。
1-3-4	网络安全政策和程序必须根据计划的时间间隔或	华为云至少每年审查一次网络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	客户应根据计划的频率或外部监管的变化定期对网络安全政策与程序进行审查和更新。

	相关法律规定的 变化定期进行审 查。更改和审查 应得到批准并记 录在案。	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。同时华 为云有专门的审计团队定期评估策 略、规程及配套措施和指标的符合 性和有效性，向最高管理层报告调 查的结果和建议。	全政策和程序进 行审查和更新，并保 留修订记录。
--	--	---	--------------------------------

5.1.4 网络安全角色与责任

确保为在组织内参与实施网络安全控制的所有各方定义角色和责任。

编号	具体控制要求	华为云的内部实践	客户的职责
1-4-1	网络安全组织结 构和相关角色和 职责应在确保不 会导致利益冲突 的同时，由授权 官员定义、记 录、批准、支持 和分配。	华为云在各产品、服务的业务团队 中明确规定了所有员工对应角色的 网络安全责任，华为云设置专门负 责安全及隐私保护的角色承担一定 的安全管理职责。网络安全相关的 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。华为云遵 循职责分离和权限制衡原则，对不 相容职责进行分离，实现合理的权 限分工，同时制定了 SOD 权责分离 管理矩阵以帮助实现该管理原则。	客户组织的负责人 或代表应定义和批 准网络安全组织架 构以及角色与职 责，确保各职责间 没有利益冲突。
1-4-2	必须根据计划的 时间间隔或相关 法律法规的变化 定期审查网络安 全角色和职责。	华为云持续监控外部监管环境的变 化，明确最新外部监管要求，对相 关的信息安全策略、流程及其角色 和职责进行审查和更新，对识别到 的法律法规的变化及时调整到内部 安全要求中，确保控制的适当性和 执行的有效性。华为将网络安全要 求融入到任职资格标准中。员工在 任职晋升过程中需要学习相应的网 络安全课程，通过相应的网络安全 技能考试，提升自身网络安全能 力。	客户应根据计划的 频率或外部监管的 变化定期对网络安 全角色与职责进行 审查和更新。

5.1.5 网络安全风险管理

确保以系统性方法管理网络安全风险，以按照组织政策、程序及相关法律法规保护组织的信息和技术资产。

编号	具体控制要求	华为云的内部实践	客户的职责
1-5-1	应根据信息和技 术资产的机密	华为云根据 IT 资产的机密性、完整 性和可用性识别资产价值，再根据	客户应根据资产的 机密性、完整性和

	性、完整性和可用性定义、记录和批准网络安全风险管理的方法和程序。	资产脆弱性和面临的威胁对资产开展安全风险评估。华为云建立了网络安全风险管理规范，明确风险管理应遵循的关键流程、风险管理范围、风险管理相关责任部门及风险管理中应遵循的标准，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断。	可用性，建立符合其组织战略的网络安全风险管理的方法和程序。
1-5-2	网络安全风险管理方法和程序应由网络安全职能部门实施。	华为云各业务团队根据要求定期执行信息安全风险评估，网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，识别有关的网络安全风险，并对风险处置跟进过程进行定期评审，确保符合公司风险管理要求。风险评估报告完成后由高级管理层进行审批。	网络安全风险管理的具体活动应由客户组织的网络安全职能部门实施。
1-5-3	网络安全风险评估程序应至少在以下方面实施： 1-5-3-1 技术项目的早期阶段。 1-5-3-2 在对技术基础设施进行重大更改之前。 1-5-3-3 在获取第三方服务的计划阶段。 1-5-3-4 在新的技术服务和产品的规划阶段和上线之前。	在项目初期对其进行信息安全风险评估并在整个项目交付过程中定期评审信息安全影响。同时，华为云制定了变更管理的管理规定和变更流程，各项变更均需通过多个环节的审核，以确保对组织的运行和安全没有负面影响。	客户应确保在技术项目的早期阶段，技术基础设施发生重大更改之前，获取第三方服务的计划阶段及新的技术服务和产品的规划阶段和上线之前开展网络安全风险评估，以保证组织信息安全的持续运行。
1-5-4	网络安全风险管理方法和程序应根据计划的时间间隔或相关法律法规的变化进行定期审查。更改和审查应得到批准并记录在案。	华为云定期评估外部监管环境的变化，明确最新外部监管要求，在风险评估过程中进行全面的检查和评估。	客户应根据计划的频率或外部监管的变化定期对网络安全风险管理方法和程序进行审查和更新，并保留修订记录。

5.1.6 信息技术项目管理中的网络安全

根据组织政策和程序以及相关法律法规，确保网络安全要求包含在项目管理方法和程序中，以保护信息和技术的机密性、完整性和可用性。

编号	具体控制要求	华为云的内部实践	客户的职责
1-6-1	作为项目管理生命周期的一部分，项目和资产（信息/技术）变更管理方法和程序中应包含网络安全的要求，以识别和管理网络安全风险。网络安全要求应是技术项目总体要求的关键部分。	华为云在项目管理中将安全目标纳入项目目标，在项目初期对其进行信息安全风险评估并在整个项目交付过程中定期评审信息安全影响。华为云制定了变更管理的管理规定和变更流程，各项变更均需通过多个环节的审核，需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保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，变更委员会审批通过后才可以上线，以更好地识别和管理网络安全风险。	客户应将网络安全要求融入项目管理及变更管理中，确保在项目管理中对识别的网络安全风险进行管理。
1-6-2	项目和资产（信息/技术）变更管理中的网络安全要求必须至少包括以下内容：	<p>1-6-2-1 漏洞评估和修复。</p> <p>华为云建立了安全漏洞管理流程，规范了华为云系统安全漏洞的预警、评估、修复处理的闭环流程，并要求了定期安全关键安全补丁，降低漏洞风险，对漏洞定级、责任分配及漏洞处理要求进行规定。同时，华为云建立了专门的漏洞响应团队，及时评估并分析漏洞的原因、威胁程度及制定补救措施，评估补救方案的可行性和有效性。华为云针对会影响客户服务的漏洞，华为云会发布漏洞公告，其中包括漏洞详情、漏洞原理分析、漏洞影响范围、漏洞防范措施及漏洞解决方法等内容。</p> <p>1-6-2-2 在技术项目变更或上线之前进行配置审查、安全配置以及加固和补丁。</p> <p>所有产品在上线前都经过了多轮安全测试，其中华为云将其深入理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具，如 SecureCat 可以对业界主流的 OS 和 DB 的安全配置进行检查。此外，产品上线前均须由安全工程实验室按照对应的安全配置规范执行检查。华为云构建了配置监</p>	<p>客户制定的项目和资产变更管理方法或程序中应包含漏洞评估和修复流程。</p> <p>客户制定的项目和资产变更管理方法或程序中应包含在技术项目变更或上线之前进行配置审查、安全配置以及加固和补丁的流程。</p>

		控平台，实现对服务器操作系统、数据库管理系统及网络设备的配置项进行实时监控。配置监控平台会将实际的配置项同标准配置基线进行对比。当出现差异时，差异分析结果会通过邮件自动发送至巡检管理员进行后续跟进处理。	
1-6-3	与软件和应用程序开发项目相关的网络安全要求应至少包括以下内容：		
	1-6-3-1 使用安全编码标准。 华为云严格遵从华为对内发布的安全编码规范。华为云服务研发和测试人员在上岗前均通过了对应规范的学习和考试。同时引入了静态代码扫描工具每日检查，其结果数据进入云服务持续集成和持续部署（CI/CD - ContinuousIntegration, ContinuousDeployment）工具链，通过质量门限进行控制，以评估云服务产品的质量。所有云产品、云服务在发布前，均需完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。	客户制定的软件开发项目管理方法或程序中应明确安全编码标准或规范。	
	1-6-3-2 为软件开发工具和库使用受信任的和许可的来源。 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。华为云对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件退出等环节，均实施严格的管控。例如在选型分析环节，增加开源软件选型阶段的网络安全评估要求，严管选型。在上线前，引入的开源软件均遵从华为公司发布的安全配置规范要求进行加固后才能应用到生产环境。在使用中，须将第三方软件作为服务或解决方案的一部分开展相应活动，并重点评估开源及第三方软件和自研软件的结合点，或解决方案中使用独立的第三方软件是否引入新的安全问题。	客户制定的软件开发项目管理方法或程序中应明确适用受信任的和许可来源的软件开发工具和库。	
	1-6-3-3 根据定义的组织网络安全要求对软件进行合规性测试。 所有云服务发布前都经过了多轮安全测试，包括但不限于 Alpha 阶段的认证、鉴权、会话安全等微服务级功能和接口安全测试，Beta 阶段通过对 API 和协议的 fuzzing 测试验证服务集成，Gamma 阶段的	客户应根据其自身的网络安全要求对软件进行合规性测试。	

		数据库安全等安全专项测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。同时，华为云将其深入理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具，如 SecureCat 可以对业界主流的 OS 和 DB 的安全配置进行检查。	
	1-6-3-4 软件组件之间的安全集成。	华为云已经采用全新的持续集成、持续交付、持续部署、快速迭代 DevOps 流程。华为云使用内部 Devops 平台来实现应用安全开发生命周期中的自动构建、测试和上线部署步骤，可防止软件在环境中传输过程中被篡改。同时引入了静态代码扫描工具每日检查，其结果数据进入云服务持续集成和持续部署（CI/CD - ContinuousIntegration, ContinuousDeployment）工具链，通过质量门限 进行控制，以评估云服务产品的质量。	客户应落实软件组件之间的安全集成。
	1-6-3-5 在软件产品上线之前进行配置审查、安全配置以及加固和修补。	新进入华为云生产环境的系统或组件，由各交付团队按照华为云已发布的安全配置规范进行自检，运维团队遵循安全配置规范对系统或组件进行加固，华为云安全运维团队负责例行抽检华为云生产环境中各系统或组件安全配置的遵从情况。	客户制定的软件开发项目管理方法或程序中应包含在软件产品上线之前进行配置审查、安全配置以及加固和补丁流程。
1-6-4	应定期审查项目管理中的网络安全要求。	华为云每年会对建立的安全开发、安全测试、配置管理等相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对项目管理中的安全要求进行审查和更新。

5.1.7 网络安全标准、法律及法规合规

应确保组织的网络安全计划符合相关法律法规。

编号	具体控制要求	华为云的内部实践	客户的责任
1-7-1	组织应遵守相关的国家网络安全	华为云在其网络安全策略中明确合规流程，定期识别和记录合规要	客户应定期识别并遵守相关国家的网

	法律法规。	求。同时，华为云设立了专岗同外部各方保持积极的联系，以追踪法律、法规的相关要求变化。当识别到与华为云服务相关的法律、法规，华为云将及时调整内部安全要求和安全控制水平，跟进对法律、法规要求的符合性。	络安全法律法规的要求。
1-7-2	组织应遵守任何国家批准的国际协议和与网络安全有关的承诺。	华为云在其网络安全策略中明确合规流程，定期识别和记录合规要求。同时，华为云设立了专岗同外部各方保持积极的联系，以追踪法律、法规的相关要求变化。当识别到与华为云服务相关的法律、法规，华为云将及时调整内部安全要求和安全控制水平，跟进对法律、法规要求的符合性。	客户应定期识别并遵守相关国家批准的国际协议和与网络安全相关的要 求。

5.1.8 定期网络安全审查与审计

确保实施网络安全控制并遵守组织政策和程序，以及相关的国家和国际法律、法规和协议。

编号	具体控制要求	华为云的内部实践	客户的责任
1-8-1	网络安全审查应由组织中的网络安全职能部门定期进行，以评估组织中网络安全控制的合规性。	华为云制定了内审管理流程，规范内部审计原则、审计管理流程和审计频率。华为云每年由专门的审计团队执行一次内部审计工作，以检查公司内部控制体系的运行情况，评估策略、规程及配套措施和指标的符合性和有效性。	客户应定期由组织内负责网络安全的职能部门进行内部审核，以确定网络安全控制的合规性和有效性。
1-8-2	网络安全审计和审查应由网络安全职能（例如内部审计职能）之外的独立方进行，以评估组织中网络安全控制的合规性。根据公认的审计标准(GAAS) 和相关法律法规，审计和审查必须独立进行，同时确保不会导致利益冲突。	华为云会定期聘请独立的外部第三方提供外部审计鉴证服务，这些评估员通过执行定期安全评估和合规性审计或检查（例如 SOC、ISO 标准、PCI DSS 审计）来评估信息和资源的安全性、完整性、机密性和可用性，从而对风险管理内容/流程进行独立评估。	客户应定期聘请外部的独立第三方对组织中网络安全控制的合规性和有效性进行审计。

1-8-3	<p>网络安全审计和审查的结果应记录在案并提交给网络安全指导委员会和授权官员。该结果应包括审计/审查范围、发现、建议和补救计划。</p>	<p>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。审计结果交由管理层进行审阅并对整改情况进行跟进。</p>	<p>审查和审计报告应提交至客户组织的网络安全委员会，其中应包含审计范围、审计发现、补救建议和补救计划等内容。</p>
-------	--	---	---

5.1.9 人力资源网络安全

确保与人员(员工和承包商)相关的网络安全风险和要求在雇佣前、雇佣期间和终止/离职后按照组织政策和程序以及相关法律进行有效管理规定。

编号	具体控制要求	华为云的内部实践	客户的责任
1-9-1	应定义、记录和批准人员网络安全要求（就业前、就业期间和终止/离职后）。	华为云建立了人员信息安全管理规定，明确了华为云各类员工分层分级的信息安全管理要求，对内外部员工关于招聘、培训、稽核和奖罚等方面管理进行了规范，明确了员工应遵循的华为云网络安全职责。	客户应制定并落实员工在雇佣前、雇佣期间及雇佣后的网络安全要求。
1-9-2	应落实人员网络安全要求。	华为云相关人员遵循华为云建立的人员信息安全管理规定，落实内外部员工在就职前、就职期间和离职后的信息安全要求。	客户应确保其员工遵循组织定义的网络安全管理要求，落实员工的信息安全要求。
1-9-3	入职前的人员网络安全要求应至少包括以下内容：		
	1-9-3-1 在雇佣合同中包含人员网络安全责任和保密条款（包括雇佣期间和终止/离职后的网络安全要求）。	员工与公司签署的聘用协议中包含保密条款，其中明确说明员工的网络安全责任，以确保在入职前对应遵循的保密条款进行确认。华为云规定员工离职时需签署离职保密承诺书，确认其应持续承担的信息安全责任及职责。	客户应在劳动合同及保密条款中包含人员应遵守的网络安全的要求。
	1-9-3-2 筛选或审查网络安全和关键/特权职位的候选人。	人员任用前，华为云通过既定的新进员工背景调查机制对满足特定条件的拟聘员工进行背景审查，同时，在适用法律允许的情况下，华为云会根据可接触的资产的机密性，在聘用员工或外部人员前对其进行背景调查。	客户应在雇佣前对涉及网络安全或关键/特权职位的候选人进行背景调查进行筛选和审查。

1-9-4	任职期间的人员网络安全要求应至少包括以下内容：		
	1-9-4-1 网络安全意识（入职和就业期间）。	华为云为确保员工的信息安全意识能够符合公司要求建立了一系列的信息安全培训及学习机制。新员工在入职后均须参加公司组织的信息安全考试，员工仅能在考试通过后才可以正式转正。针对在职员工，在员工在职期间持续进行，华为云每年定期组织信息安全意识培训、信息安全知识宣传。	客户应对定期对在职员工进行网络安全培训。
1-9-5	1-9-4-2 根据组织的网络安全政策与程序实施和遵守网络安全要求。	华为云定期开展网络安全意识教育学习，要求员工持续学习网络安全知识，了解相关的政策和制度，知道哪些行为是可以接受，哪些是不能接受的，意识到即使主观上没有恶意，也要对自己的行为负责，并承诺按要求执行。同时，华为云建立了严密的安全责任体系，贯彻违规问责机制。华为云以行为和结果为主要依据对员工进行问责。	客户应确保在员工应根据已定义的网络安全政策和程序执行其职位所需遵循的网络安全要求。
1-9-6	人员对信息和技术资产的访问应在终止/离职后立即进行审查和删除。	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。	客户应确保在员工离职后对其相关权限和资产进行审查和回收。

5.1.10 网络安全意识和培训计划

应确保人员了解其网络安全责任并具备基本的网络安全意识。还需确保为人员提供必要的网络安全培训、技能和证书，以帮助完成其网络安全职责并保护组织的信息和技术资产。

编号	具体控制要求	华为云的内部实践	客户的责任
1-10-1	应制定和批准网络安全意识计划。该计划必须	华为云建立了培训机制，以提高员工的信息安全意识，根据不同的角色、岗位为员工设计合适的培训方	客户应制定完善的安全意识和技能培训管理机制，根据

	通过多种渠道定期开展，以增强对网络安全、网络威胁和风险的认识，建立积极的网络安全意识文化。	案。制定了专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课、信息安全宣讲、案例学习等。	培训对象的职能和角色来制定培训内容，定期分析并更新培训内容。
1-10-2	应实施网络安全意识计划。	华为云遵循制定的信息安全意识培训计划，在员工在职期间持续对员工的安全意识教育进行培训，培养员工安全意识，以提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营。	客户应遵循制定的网络安全意识培训计划，对员工进行安全意识教育培训。
1-10-3	网络安全意识计划必应涵盖最新的网络威胁及如何防范威胁，并且应至少包括以下主题： 1-10-3-1 安全处理电子邮件服务，尤其是钓鱼电子邮件。 1-10-3-2 移动设备和存储介质的安全处理。 1-10-3-3 安全的互联网浏览。 1-10-3-4 安全使用社交媒体。	华为云为确保员工的信息安全意识能够符合公司公司要求建立了一系列的网络安全培训及学习机制，要求员工持续学习网络安全知识，了解相关的政策和制度，会涵盖安全处理钓鱼邮件、移动设备和存储介质的安全处理、安全的互联网浏览及安全使用社交媒体等主题。；面向全员开展形式多样的网络安全宣传活动，包括网络安全社区运营、网络安全典型案例宣传、网络安全活动周、网络安全动画宣传片等，以提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营。	客户制定的网络安全意识计划应涵盖最新的网络威胁及如何防范这些威胁。
1-10-4	应向直接从事与网络安全相关任务的人员提供必要的和定制的（即针对与网络安全相关的工作职能量身定制）培训和专业技能组合，包括： 1-10-4-1 网络安全部门的人员。 1-10-4-2 从事软件/应用程序开发的人员，以及信息和技术资产运	华为云建立了自己的培训机制，根据不同的角色、岗位为员工设计合适的培训方案。其中一般员工的培训频率为至少每年一次，核心岗位员工培训频率更高。华为云对开发人员、运维工程师及网络安全管理人员等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。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。	客户应向直接从事与网络安全相关的人员提供必要的和定制的培训和专业技能组合。

	营。 1-10-4-3 执行和监督岗位。		
1-10-5	应定期审查网络安全意识计划的实施情况。	华为云每年会对建立的人员意识培训计划进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对网络安全意识计划的实施情况进行审查。

5.2 网络安全防御

“网络安全防御”中要求客户制定网络安全运营和安全管理的策略及流程，包括资产管理、身份与访问管理、信息系统与信息处理设施的保护、密码管理、备份与恢复、网络安全事件管理等方面。相关控制要求及华为云的实践方式如下：

5.2.1 资产管理

确保组织拥有准确和详细的信息和技术资产清单，以支持组织的网络安全和运营要求并维护信息和技术资产的机密性、完整性和可用性。

编号	具体控制要求	华为云的内部实践	客户的责任
2-1-1	应定义、记录和批准管理信息和技术资产的网络安全要求。	华为云制定了资产管理程序，明确了信息资产的分级定级办法以及针对各类资产应遵循的授权规则，同时也建立了信息资产保密管理要求，明确华为云对各级别信息资产应采取的保密措施，规范使用资产的行为，使公司资产得到合理保护和共享。	客户应建立正式的资产管理程序，对其资产进行分类，并定义资产所有者。
2-1-2	应实施管理信息和技术资产的网络安全要求。	华为云定期对华为云的硬件、软件、数据、人员和服务进行识别。华为云通过资产管理系统（Cloud Asset Management）实时监控资产管理平台中记录的华为云平台的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。此外，华为云设置配置经理对所有业务单元进行配置管理，资源配置模型分为主机、服务树、云基础设施和网络设备，通过构建配	客户应遵循已建立的资产管理程序，编制和维护资产清单，对不同类别的资产采取适用的保护措施。 华为云的企业主机安全（Host Security Service，简称 HSS）为客户提供统一的管理界面，供客户查询

		置项映射和资源生命周期管理，支撑现网运维获得的稳定和安全，并通过专业的配置管理数据库工具（CMDB）对配置项、配置项的属性和配置项之间的关系进行管理。华为云并使用 IPAM 对 IP 资源进行统一的管理。同时，华为云平台部署了 HSP 主机安全平台套件，对平台资产进行网络安全防护。	并管理云服务，是服务器的贴身安全管家，为客户提供资产管理功能，包括提供账号、端口、进程、Web 目录和软件等安全资产信息的管理和分析。
2-1-3	应定义、记录和批准信息和技术资产的可接受使用政策。	华为云已制定并实施资产的使用规则，包括管理原则、相关人员职责、办公计算机安全要求、办公网络安全要求、办公应用系统安全要求、存储介质与端口安全要求、办公外设安全要求、非华为计算机安全要求以及相关违规的处罚等。	客户应定义定资产的可接受使用规则，包括但不限于办公终端的安全使用规范、存储介质的安全要求、办公网络的安全使用规范等。
2-1-4	应实施信息和技术资产的可接受使用政策。	华为云实施资产的使用规则，包括管理原则、相关人员职责、办公计算机安全要求、办公网络安全要求、办公应用系统安全要求、存储介质与端口安全要求、办公外设安全要求、非华为计算机安全要求以及相关违规的处罚等。	客户应遵循已制定的资产的可接受使用规则，对办公终端、存储介质、办公网络等资产实施安全管理措施。
2-1-5	信息技术资产应按照相关法律和监管要求进行分类、标记和处理。	华为云通过资产管理系统（Cloud Asset Management, CAM）实施监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。此外，华为云设置配置经理对所有业务单元进行配置管理，资源配置模型分为主机、服务树、云基础设施和网络设备，通过构建配置项映射和资源生命周期管理，支撑现网运维获得的稳定和安全，并通过专业的配置管理数据库工具（CMDB）对配置项、配置项的属性和配置项之间的关系进行管理。同时，华为云对数据进行分级管理，结合机密性、完整性、可用性、合规性进行综合定级，将数据分为多个安全级别并分别给出该级别数据的定义。同时规定了不同级别数据的安全实施要求、稽查要求以及应急响应及演练要求。各业务领域遵照数据定级标准对其领域内数据标	客户应依照法律要求、资产价值、资产对组织的重要性以及敏感性标注相应资产的分类，并依据不同级别的资产分类定义和制定信息和技术资产管理的网络安全要求，确保资产按照其对组织的重要程度受到适当水平的保护。

		记安全等级。	
2-1-6	应定期审查管理信息和技术资产的网络安全要求。	华为云每年会对建立的资产管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对信息和技术资产的网络安全要求进行审查和更新。

5.2.2 身份与访问管理

确保对信息和技术资产的安全且受限制的逻辑访问，以防止未经授权的访问，并仅允许完成分配任务所必需的用户进行授权访问。

编号	具体控制要求	华为云的内部实践	客户的责任
2-2-1	应定义、记录和批准身份和访问管理的网络安全要求。	华为云制定了公司用户账号权限管理的要求，规范华为云员工在申请、维护和注销权限时应遵循的流程。此外，针对华为云云平台账号，华为云制定了公有云账号权限管理要求及流程，明确了对账号的分类管理和访问控制策略，相关文件均通过评审流程并发布。	客户应建立身份认证与访问控制管理机制，对访问系统的行为进行权限限制和监督。
2-2-2	应实施身份和访问管理的网络安全要求。	华为云员工在内部办公网络中使用唯一身份标识，已建立完善的账号生命周期管理规定及流程。对云服务的访问通过统一身份认证服务（IAM - Identity and Access Management）对用户进行访问控制和权限管理。所有运维账号，设备及应用的账号均进行统一管理，以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。	客户应遵循已建立的身份认证与访问控制管理策略，对用户账号进行权限管控。 客户可通过华为云的统一身份认证服务（Identity and Access Management，简称 IAM）对使用云资源的用户账号进行管理。华为云统一身份认证服务提供适合企业级组织结构的用户账号管理服务，为客户分配不同的资源及操作权限。
2-2-3	身份和访问管理的网络安全要求应至少包括下列的：		
	2-2-3-1 基于用户	华为云员工在内部办公网络中使用	客户应使用基于用

	名和密码的用户认证。	唯一身份标识，已建立完善的账号生命周期管理规定及流程。新员工入职须经过用人部门总裁及部门 HR 的审批授权，管理平台会在审批后为该员工创建一个账号，该账号为员工在华为云内部各系统或平台中登录所用账号。华为云所有运维账号实现统一管理，并通过统一审计平台集中监控，并且进行自动审计。运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一身份标识的员工身份账号，且要求使用双因子认证。	户名和密码的用户认证策略。 华为云统一身份认证服务支持密码认证，客户通过使用访问密钥获得基于统一身份认证服务的认证和鉴权后，以调用 API 的方式访问云资源。
	2-2-3-2 远程访问的多因素身份验证。	华为云使用 IAM 对访问进行管理，支持多因素认证用于登录验证和操作保护，员工每次登陆均需要使用多重身份验证确定身份。员工通过互联网访问华为云办公网时须通过支持注册认证的设备及账号密码双因素认证的虚拟专属网络（VPN）方可登录认证。此外，运维人员接入华为云管理网络对系统进行集中管理时，需使用员工身份账号，且要求使用双因子认证，如 USB key、Smart Card 等。员工账号用于登录 VPN、堡垒机，实现用户登录的深度审计。	客户应对远程访问进行多因素身份验证策略。 客户可使用华为云统一身份认证服务，在密码认证通过后，还将收到一次性短信验证码进行二次认证。修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。
	2-2-3-3 基于身份和访问控制的用户授权原则：需知、按需使用、最小特权和职责分离。	华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访问。	客户应实施基于角色的访问控制及权限管理，符合按需知晓和使用的最小原则。 客户可使用华为云统一身份认证服务，可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。
	2-2-3-4 特权访问	华为云针对特权账号制定了管理要	客户应建立特权账

	管理。	<p>求，将特权账号分类并在特权账号创建、回收、授权、使用、注销等各阶段中遵守管理要求。华为云强调员工云服务账号的安全风险可控，严格要求安全强口令，定期审视账号权限范围，特权账号被严格纳管回收。</p> <p>特权账号管理系统将日常或应急运维的功能账号或技术账号绑定到运维团队或个人。仅在员工职责所需时，对其授予特权或应急账号。所有特权或应急账号的申请需要经过多级的评审和批准。华为云仅会在得到客户授权后登录租户的控制台或者资源实例协助客户进行维护。堡垒机上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人。</p>	<p>号的管理机制，密切监督特权账号的使用。</p> <p>客户可通过华为云统一身份认证服务可以更有效地细化管理特权账户。客户也可通过云审计服务（Cloud Trace Service，简称 CTS）作为辅助，CTS 为客户提供云服务资源的操作记录，供用户查询、审计和回溯使用。</p>
	2-2-3-5 定期审查用户的身份和访问权限。	华为云已规定对不同级别账号/权限的最长审视周期，账号/权限责任人会定期审视其持有的账号/权限，在使用人转岗或角色变化时由责任人提交注销申请。针对外包合作人员账号/权限，管理负责人在外包合作人员离场或不再需要账号/权限时提交注销申请。主管会审视下属的账号/权限持有情况是否合理，如下属岗位/角色变动，将审视其原有岗位账号/权限是否已注销。	客户应定期审视账号权限范围，确保用户权限申请、变更或回收时，均可以按照身份和访问控制策略进行及时的管理。
2-2-4	应定期审查身份和访问管理的网络安全要求的实施情况。	华为云每年会对建立的身份与访问管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对身份与访问管理的网络安全要求进行审查和更新。

5.2.3 信息系统与信息处理设施保护

应确保保护信息系统和信息处理设施（包括工作站和基础设施）免受网络风险。

编号	具体控制要求	华为云的内部实践	客户的责任
2-3-1	应定义、记录和批准保护信息系统和信息处理设	华为云遵循华为公司建立的 IT 安全标准，其中明确了为防止对基础设施未经授权的变更或恶意入侵而实	客户应定义保护信息系统和信息处理设施的网络安全要

	施的网络安全要求。	施的安全控制要求，包含有害代码防护、恶意软件防护、病毒防护、介质管理以及补丁管理的相关要求。	求，包含有害代码防护、恶意软件防护、病毒防护、介质管理以及补丁管理等。
2-3-2	应实施保护信息系统和信息处理设施的网络安全要求。	华为云的相关人员遵循华为公司的IT安全标准，部署防病毒软件、防火墙、IPS、IDS等一系列的网络安全防护设备，同时实施有效的安全措施保障信息处理设施的安全性。	客户应遵循已建立的信息系统和信息处理设施保护的网络安全要求，部署网络安全防护设备，实施有效的安全措施。
2-3-3	保护信息系统和信息处理设施的网络安全要求应至少包括以下内容：		
	2-3-3-1 对服务器和工作站上的恶意软件和病毒防护进行高级、最新和安全的管理。	在物理主机层面，通过部署防病毒软件，以实现对恶意软件的攻击防御。华为云桌面终端标准镜像内默认提供防病毒软件，员工默认无法对防病毒软件进行禁用操作。 此外，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。	客户应实施安全管理措施，检测和预防信息系统与信息处理设施（如服务器和工作站）上的恶意软件和恶意病毒。 客户可使用华为云的企业主机安全（Host Security Service，简称HSS），通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别病毒、木马、后门、蠕虫和挖矿软件等恶意程序，并提供一键隔离查杀能力。
	2-3-3-2 限制使用和安全处理外部存储介质。	华为云制定并实施移动介质管理规定，各类移动介质由专人管理，借用时需要审批，使用完毕后须进行格式化处理。对个人存储介质及数字设备进出不同安全保密级别的区域及其使用均制定了不同的安全要求。个人存储介质及数字设备进出不同安全保密级别的区域及其使用均制定了不同的安全要求，未经授权，不得私自使用任何存储介质连接服务器。此外，华为云也制定了存储介质及设备进出机房管理规	客户应实施保护措施以限制使用和安全处理外部存储介质，防止未经授权的介质使用而造成数据泄露风险。

		定，要求存储介质及设备进出机房前需进行登记并得到授权。物理存储介质进出机房时均会进行数据防泄漏管理，并对数据擦除、报废清退流程进行规定，减少可能存在的数据泄露损失。	
	2-3-3-3 信息系统、软件和设备的补丁管理。	华为云建立安全补丁管理的流程，保证安全补丁在 IT 安全标准规定的期限内完成安装。同时，华为云制定了漏洞管理机制，确保对云平台及云服务安全漏洞及时的应急响应，不断优化云平台及云产品默认安全配置、及时在规定的期限内应用修补措施或补丁、补丁装载前置于研发阶段和灵活简化安全补丁部署周期等。	客户应建立有效的补丁和漏洞管理机制，对所有技术资产进行漏洞识别和风险评估，对关键补丁进行测试，制定补丁更新周期以及补丁修复的工作流程。 华为云镜像服务(IMS)简单方便的镜像自助管理功能。客户可通过服务控制台或 API 对自己的镜像进行管理。华为云负责公共镜像的定期更新与维护向用户提供安装安全补丁的公共镜像和相关安全加固和补丁信息以便用户在部署测试、故障排除等运维活动时参考。
	2-3-3-4 与准确且值得信赖的来源（例如，沙特标准、计量和质量组织 (SASO)）进行集中式时钟同步。	华为云使用标准 NTP4.2.8 协议对系统内的时间进行集中式的时钟同步。同时华为云也相应客户的需求，与客户提供的来源进行集中式时钟同步。	客户应确保组织或安全域内的所有相关信息处理系统的时钟应使用准确且值得信赖的来源时钟源进行同步。
2-3-4	应定期审查保护信息系统和信息处理设施的网络安全要求。	华为云每年会对建立的 IT 安全规范，包含恶意软件防护、病毒防护、介质管理以及补丁管理等策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对保护信息系统和信息处理设施的网络安全要求进行审查和更新。

5.2.4 电子邮件保护

应确保保护组织的电子邮件服务免受网络风险。

编号	具体控制要求	华为云的内部实践	客户的责任
2-4-1	应定义、记录和批准保护电子邮件服务的网络安全要求。	华为云遵循华为公司建立的办公应用系统安全，其中明确了 Email 系统、移动邮件使用的安全控制要求，其中对邮件的收发规则及权限等进行了定义。	客户应制定和实施电子邮件服务的网络安全要求。
2-4-2	应实施电子邮件服务的网络安全要求。	华为云的相关人员遵循华为公司针对 Email 系统及移动邮件使用的安全控制要求，避免华为云的业务信息被未经授权的外发造成信息泄露等安全风险。	客户应遵循已制定的电子邮件服务的网络安全要求，实施必要的安全措施确保业务信息不会被外发从而造成数据泄露的风险。
2-4-3	保护电子邮件服务的网络安全要求应至少包括以下内容：		
	2-4-3-1 使用先进和最新的电子邮件保护技术分析和过滤电子邮件（特别是钓鱼电子邮件和垃圾邮件）。	华为云使用经由华为公司批准的技术手段，如部署防病毒程序，在邮件网关对邮件进行监测和过滤，拦截病毒邮件和垃圾邮件。	客户应使用适当的技术手段，对电子邮件进行监测和过滤。
	2-4-3-2 远程和网络邮件访问电子邮件服务的多因素身份验证。	华为云员工使用其 W3 账号登录华为云内部邮箱系统，支持多因素认证用于登录验证和操作保护，员工每次登录均需要使用多重身份验证确定身份。	客户应在远程和网络邮件访问电子邮件服务时，启用多因素身份验证策略。
	2-4-3-3 电子邮件归档和备份。	华为云规定所有反映华为公司工作活动且具有查考利用价值的电子邮件均属于归档和备份范围，且数据保留在在线存储介质上。	客户应定义电子邮件归档和备份的策略，定期对电子邮件进行备份。
	2-4-3-4 通常利用零日病毒和恶意软件对高级持续性威胁 (APT) 安全管理和防护。	华为云在其办公网络部署了 IPS 入侵防御系统、Web 应用防火墙 (WAF -Web Application Firewall)、防病毒软件等恶意软件和病毒防护系统保护电子邮件系统。华为云桌面终端标准镜像内默认提供防病毒软件，员工默认无法对防病毒软件进行禁用操作。	客户应部署针对零日病毒和恶意软件的高级持续威胁的安全防护设备。
	2-4-3-5 验证组织的电子邮件服务	华为云实施了验证组织的电子邮件服务域，防止电子邮件地址免受欺骗。	客户应实施验证组织的电子邮件服务

	域（例如，使用发件人策略框架 (SPF)）。	骗、垃圾邮件和网络钓鱼之类的恶意活动的侵害。	域的策略。
2-4-4	应定期审查电子邮件服务的网络安全要求。	华为流程 IT 网络安全部门每年会对建立的电子邮件管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对电子邮件服务的网络安全要求进行审查和更新。

5.2.5 网络安全管理

应确保保护组织的网络免受网络风险。

编号	具体控制要求	华为云的内部实践	客户的责任
2-5-1	应定义、记录和批准网络安全管理的网络安全要求。	华为云遵循华为公司建立的网络安全管理规定，其中明确了网络隔离、网络接入安全、网络安全防御等相关控制要求，确保组织免受网络恶意入侵造成网络安全风险。	客户应建立正式的系统以及网络管理程序，确保组织的网络免受安全风险。
2-5-2	应落实网络安全管理的网络安全要求。	华为云遵循网络安全管理规定，实施正式的环境隔离机制，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次安全隔离。同时华为云构建了多层次防护措施，如使用接入控制和边界防护技术以实现对外来攻击的统筹防护，严格执行相应的管控措施，确保华为云安全。	客户应落实网络安全管理的安全要求，构建网络安全防护，保障组织网络的安全性。 华为云可帮助客户构建网络安全防护体系，保障客户云服务的安全。在互联网边界客户可通过部署 Anti-DDoS 流量清洗服务，来完成对异常和超大流量攻击的检测和清洗；通过虚拟私有云（Virtual Private Cloud，简称 VPC）对关键网络分区进行划分和隔离；部署 Web 应用防火墙（Web Application Firewall，简称 WAF）对 Web 应用提供安全防护。

		Firewall, 简称 WAF) 应对 Web 攻击以保护部署在 DMZ 区、面向外网的 Web 应用服务和系统。	
2-5-3	<p>网络安全管理的要求应至少包括以下内容:</p> <p>2-5-3-1 使用防火墙和纵深防御原则对网段进行逻辑或物理隔离和分段。</p> <p>2-5-3-2 生产、测试和开发环境之间的网络隔离。</p> <p>2-5-3-3 安全浏览和互联网连接，包括限制使用文件存储/共享和远程访问网站，以及防范可疑网站。</p> <p>2-5-3-4 使用强认证和加密技术的无线网络保护。在将任何无线网</p>	<p>华为云基于业务功能及风险等级将生产及非生产环境划分为多个安全区域，DMZ 区、公共服务区（Public Service）、资源交付区（POD - Point of Delivery）、数据存储区（OBS - Object - Based Storage）、运维管理区（OM - Operations Management）。除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能，确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的 OM 区，攻击面最小，安全风险相对容易控制。</p> <p>华为云建立了正式的环境隔离机制，对开发环境、测试环境及生产环境实现严格的逻辑隔离，提升面对外部入侵和内部违规操作的自我保护和容错恢复能力，降低对运行环境未授权访问或变更的风险。禁止未经授权打通测试环境和生产环境的网络链接，避免因测试环境被入侵而导致生产环境安全风险。</p> <p>华为云制定了相关安全管理规定，其中明确用户在未经授权批准的情况下，禁止通过 Proxy 登录（华为 Email 之外的）私人电子邮箱，禁止通过网络向华为办公网络之外传送华为信息，禁止使用任何方式绕过 Proxy 限制向公司外传送数据或访问未授权的网站。同时也禁止设置所有人访问权限的共享目录。</p> <p>华为云使用强认证和加密技术的无线网络保护，同时华为云所有接入华为内部网络包括有线办公网络和无线办公网络的计算机设备均必须</p>	<p>客户需对其网络进行安全区域划分和隔离，针对不同安全域之间的访问进行严格的管控。</p> <p>客户应该保证其开发、测试和生产环境相互隔离，并严格管控不同环境的使用。</p> <p>客户应规范互联网链接和浏览的安全，限制使用文件共享存储的网站，避免远程访问网站，防范可疑网站。</p> <p>客户应实施强认证和加密技术的无线网络保护，确保在任何无线网络接入</p>

	络连接到组织的内部网络之前，必须进行全面的风险评估和管理活动以评估和管理网络风险。	安装公司安全软件，员工可通过公司安全软件从外部网络接入华为内部办公网络。此外，未经批准，在华为办公区域内，不允许接入非华为提供的无线网络，禁止在华为办公区域私自搭建无线网络或将测试无线网络接入公司办公网络，若有业务需求，必须经过业务主管和 IT 管理部门评估和审核批准。	内网之前，对其进行全面的风险评估。
2-5-3-5 网络服务、协议和端口的管理和限制。	华为云通过配置防火墙策略限制对高危端口及高危协议的使用。同时华为云内部制定了产品通信矩阵，其中对可使用的通信端口进行了维护，端口必须限定确定的合理的范围，且未在矩阵中的端口必须关闭，并通过端口扫描工具验证。	客户应制定安全管理策略限制对高危端口及高危协议的使用。	
2-5-3-6 入侵防御系统 (IPS)。	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。	客户应在网络边界部署 IPS 设备。 客户可使用华为云的企业主机安全 (Host Security Service, 简称 HSS)，HSS 包含入侵检测功能，可识别并阻止入侵主机的行为，实时检测主机内部的风险异变，检测并查杀主机中的恶意程序，识别主机中的网站后门等。	
2-5-3-7 域名服务 (DNS) 的安全性。	华为云 DNS 基于华为云高可用性和可靠性的基础架构构建，其服务器的分布式特性有助于提高可用性，确保将最终用户路由到应用程序。在单个业务节点发生故障时，可通过修改 DNS 解析记录进行故障转移，保障租户业务的可用性。华为云 DNS 具备三层攻击防护机制，首先，在运营商的骨干网部署了专业高防设备，保护 IP 地址，对异常流量进行清洗；其次，在华为云的边界处部署了 Anti-DDoS 对访问流量进行特征模拟，清洗攻击流量，限流和屏蔽恶意 IP 访问，保障服务安全稳定运行；最后，在 DNS 节点支持 ACL 阻断，可对异常 IP 和流	客户应确保域名服务 (DNS) 的安全性。 客户可使用华为云云解析服务 (DNS - Domain Name Service)，华为云 DNS 提供高可用、高扩展的权威 DNS 服务和 DNS 管理服务，同时提供 Anti-DDoS 功能，对访问流量进行特征模拟，清洗攻击流量，限流和	

	量进行阻断拉黑。华为云遵循内部安全操作规范，定期对 DNS 的版本进行升级更新，确保 DNS 的可用性以及配置的安全性。	屏蔽恶意 IP 访问，保障服务安全稳定运行。
2-5-3-8 安全管理和保护 Internet 浏览通道免受高级持续威胁 (APT) 的攻击，这些威胁通常利用零日病毒和恶意软件。	华为云使用 IPS 入侵防御系统、Web 应用防火墙 (WAF-Web Application Firewall)、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。	客户应实施安全管理策略以保护 Internet 浏览通道免受高级持续威胁的攻击。 客户可使用华为云的企业主机安全 (Host Security Service, 简称 HSS)，通过程序特征、行为检测，结合 AI 图像指纹算法以及云查杀，有效识别病毒、木马、后门、蠕虫和挖矿软件等恶意程序，并提供一键隔离查杀能力。同时，客户可部署华为云 Web 应用防火墙 (Web Application Firewall, WAF) 对网站业务流量进行多维度检测和防护。Web 应用防火墙可结合深度机器学习智能识别恶意请求特征和防御未知威胁，通过对 HTTP(S) 请求进行检测，识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，全面避免网站被黑客恶意

			攻击和入侵，保护 Web 服务安全稳定。
2-5-4	应定期审查网络安全管理的网络安全要求。	华为云每年会对建立的网络管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对网络安全的安全要求进行审查和更新。

5.2.6 移动设备安全

应确保保护移动设备（包括笔记本电脑、智能手机、平板电脑）免受网络风险，并确保利用自带设备 (BYOD) 政策的同时安全处理组织的信息（包括敏感信息）。

编号	具体控制要求	华为云的内部实践	客户的责任
2-6-1	应定义、记录和批准移动设备安全和 BYOD 的网络安全要求。	华为云制定了移动设备管理规定，以实施对移动计算设备的统一管理。对移动设备使用的原则、职责、权限要求、设备管理安全要求、网络接入要求及违规处罚等均做出规定。	客户应制定移动设备安全和 BYOD 管理策略。
2-6-2	应实施移动设备安全和 BYOD 的网络安全要求。	华为云员工遵循华为云移动设备管理规定，履行规范中针对移动设备使用的安全要求，保障移动办公终端上的公司数据的信息安全，对资产的使用负责。	客户应遵循已定义的移动设备和 BYOD 的安全管理策略，保障移动设备上数据的安全性。
2-6-3	移动设备安全和 BYOD 的网络安全要求应至少包括以下内容：		
	2-6-3-1 存储在移动设备和 BYOD 上的组织数据和信息的分离和加密。	华为云建立了保护技术设备上的数据的加密策略与密钥管理机制，对人员的权限与职责分配、加密级别、加密方法进行了规定。同时，针对不同级别的数据，限制含有涉密数据的电子流或邮件发布到移动 BYOD 端的应用中，BYOD 上的组织数据和信息不涉及华为的核心信息资产。	客户应确保对存储在设备中的数据和信息资产进行加密和分离措施。
	2-6-3-2 根据工作要求控制和限制使用。	华为员工的办公计算机由华为公司统一配备，针对便携电脑，机要岗位不配备便携电脑，当便携电脑进入受控区域时需获得批准，同时对	客户应根据设备使用者的工作角色和权限管理和限制对移动设备的使用。

		便携电脑采取措施以防止丢失后发生数据泄露（例如设置硬盘保护密码或安装全硬盘加密软件等）。此外，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，并按照员工权限对应用程序的访问范围进行控制。	
	2-6-3-3 在设备丢失、被盗或与组织终止/分离后，安全擦除存储在移动设备和 BYOD 上的组织数据和信息。	员工离职或转岗等，必须对办公计算机硬盘进行格式化处理，若涉及机密、绝密信息，应确保删除的数据无法恢复，同时主动及时的卸载 BYOD 上公司应用清楚公司数据。若设备丢失或被盗，员工须向业务主管和信息安全部门报告，并远程擦除公司数据，并取消设备绑定。	客户应在设备丢失、被盗或与组织终止/分离后，安全清除存储在移动设备和 BYOD 上的组织数据和信息。
	2-6-3-4 移动设备用户的安全意识。	在培养员工安全意识方面，华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。	客户应定期对使用移动设备的员工进行安全意识培训，对移动设备的安全使用和责任进行宣贯。
2-6-4	应定期审查移动设备安全和 BYOD 的网络安全要求。	华为云每年会对建立的移动办公终端相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对移动设备和 BYOD 的安全要求进行审查和更新。

5.2.7 数据和信息保护

根据组织政策和程序以及相关法律法规，确保组织数据和信息的机密性、完整性和可用性。

编号	具体控制要求	华为云的内部实践	客户的责任
2-7-1	应根据相关法律法规定义、记录和批准保护和处理数据和信息的网络安全要求。	华为云制定了数据安全策略及数据安全保护管理规定，对数据资产的分级分类标准进行了定义，同时明确了数据匿名化及标签化处理标准，对数据在整个生命周期中须遵循的安全措施进行了规范。同时，华为云制定了云服务安全与隐私活动操作指导，规范云服务在产品生命周期中应遵循的隐私保护要求。	客户应建立正式的数据保护机制，对信息的全生命周期进行保护。

2-7-2	应实施保护和处理数据和信息的网络安全要求。	华为云实施数据安全相关控制措施，华为云还设计和实施一系列对数据安全和信息生命周期管理的技术措施和管理程序，以确保用户安全。	客户应实施适当的数据和信息保护措施，保障数据在存储、处理和传输过程的安全性。
2-7-3	保护和处理数据和信息的网络安全要求应至少包括以下内容：		
2-7-3-1	数据和信息所有权。	华为云作为云服务提供商，定义了华为云数据安全责任共担模型。在与客户签订的用户协议中明确划分了客户与华为云数据的所有权、安全责任和义务。对于客户内容数据，华为云承诺不触碰客户的内容数据。对于客户的采购相关的信息，华为云将依照数据保留条款、隐私声明等协议予以保护，在处理过程中，遵循数据最小化原则收集、存储和使用客户的信息，并通过全面的数据保护措施确保客户的账户信息安全。	客户是其数据的所有者和控制者。客户应确保其内容数据的保密性、完整性、可用性，并对数据访问的身份验证和鉴权进行有效保障。
2-7-3-2	数据和信息分类和标记机制。	华为云对数据进行分级管理，结合机密性、完整性、可用性、合规性进行综合定级，将数据分为多个安全级别并分别给出该级别数据的定义。同时规定了不同级别数据的安全实施要求、稽查要求以及应急响应及演练要求。各业务领域遵照数据定级标准对其领域内数据标记安全等级。	客户应依据数据和信息的重要性和机密性等要素制定分类标准并遵循规定的分类标准对数据进行分类和标记。 客户可使用华为云的数据安全中心服务（DSC - Data Security Center）是新一代的云原生数据安全平台，可以为客户提供数据分级分类、数据安全风险识别、数据水印溯源、数据脱敏等基础数据安全能力，并通过数据安全总览整合数据安全生命周期各阶段状态，对外整体呈现云上数据安全态势。
2-7-3-3	数据和信息隐私。	华为云以全球隐私保护的法律法规为基石，参考业界广泛认可的优秀实践，建设了华为云的隐私保护体系，对隐私和个人可识别信息进行	客户应正确、全面地识别云端的个人数据，制定可保护个人数据的安全及

		保护。华为云建立了一系列数据保护措施，以确保数据和信息的安全性。为更好地保障数据主体权利与保护个人数据安全，华为云将个人数据处理基本原则贯彻到个人数据处理各个阶段，明确个人数据处理全生命周期的管控要求，并将这些要求融入到所有业务活动中。	隐私的策略并选择恰当的隐私保护措施，保障个人数据、隐私数据或机密数据的安全。
2-7-4	应定期审查保护和处理数据和信息的网络安全要求。	华为云每年会对建立的数据安全及隐私安全相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对保护数据和信息安全的网络安全要求进行审查和更新。

5.2.8 密码学

根据组织政策和程序以及相关法律法规，确保正确有效地使用密码学来保护信息资产。

编号	具体控制要求	华为云的内部实践	客户的责任
2-8-1	应定义、记录和批准密码学的网络安全要求。	华为云制定并实施密码算法应用规范，介绍了如何选择安全的加密算法以及使用安全加密算法时的规则，并结合应用实例指导正确使用密码算法。	客户应建立密码管理政策，确保正确有效地使用密码学来保护信息资产。
2-8-2	应实施密码学的网络安全要求。	华为云自身使用行业广泛使用的AES强效加密法对平台内的数据进行加密，在传输过程中使用高版本TLS加密协议保障数据安全，确保不同状态下的数据的机密性。使用数字签名和时间戳等控制机制，防止数据传输过程中被篡改，确保信息完整性并防止重放攻击。	客户应确保适当和有效地使用密码技术以保护信息的保密性、真实性和完整性。
2-8-3	密码学的网络安全要求应至少包括以下内容：		
	2-8-3-1 批准的密码解决方案标准及其技术和监管限制。	华为云实施由华为云网络安全能力中心维护的密码算法应用规范，其中包含常见密码算法及方案的标准化信息列表，此列表已参考业界广泛采用标准和最佳实践，指导产品正确选择和使用密码算法。	客户在使用加密措施保护数据时，应考虑采用业内认可的加密算法和密钥管理机制。
	2-8-3-2 加密密钥	华为云制定并实施密钥管理安全规	客户应建立密钥管

	在其生命周期内的安全管理。	范，对密钥生命周期各阶段的安全进行管理，明确在密钥生成、传输、使用、存储、更新、备份与恢复、销毁等阶段的安全管理要求。	理机制，用于处理加密密钥的生成、保护、归档、恢复和销毁，使数据的机密性和完整性不会受到损害。 华为云为客户提供了数据加密服务(DEW)，其密钥管理功能可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，助力客户云上数据的安全。 DEW 采用分层密钥管理机制，方便各层密钥的轮换。华为云使用的硬件安全模块(HSM)为客户创建和管理密钥，HSM 拥有 FIPS140-2(2 级和 3 级)的主流国际安全认证，助力用户的 data 合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取客户根密钥。DEW 还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业务的无缝集成、对接。同时，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机制，保障了密钥的持久性。
	2-8-3-3 根据分类和相关法律法规	华为云建立了保护技术设备上的数据的加密策略与密钥管理机制，对	客户应定义密码的使用策略，依据数

	对传输中和静态数据进行加密。	加密级别、加密方法进行了规定。华为云自身使用行业广泛使用的AES强效加密法对平台内的数据进行加密。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，传输中数据的保护通过如下方式提供： 1. 虚拟专用网络（VPN）：用于在远端网络和VPC之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云。目前，华为云采用硬件实现的IKE（密钥交换协议）和IPSecVPN结合的方法对数据传输通道进行加密。 2. 应用层TLS与证书管理：华为云服务提供REST和Highway方式进行数据传输。 以上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。 此外，华为云提供的基础设施存储、数据库本身具有数据备份的机制，备份的数据副本和数据采用同样的数据安全措施。例如云硬盘提供安全的加密算法（AES-256）和功能、对象存储服务可提供服务端加密功能及防盗链功能、RDS数据库提供存储加密机制等。通过与数据加密服务集成，备份数据可以方便、快速地实现加密存储，有效保证备份数据的安全性。	据和信息的分类级别，考虑对传输中和静态数据的加密算法的类型、强度和质量。 客户可通过华为云的数据加密服务DEW实现对数据的加密，华为云将复杂的数据加解密、密钥管理逻辑进行封装，使得客户的数据加密操作变得简单易行。 目前，华为云云硬盘（EVS）、对象存储服务（OBS）、镜像服务（IMS）和关系型数据库等多个服务均提供数据加密（服务端加密）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。 对于传输中的数据，当客户通过互联网提供Web网站业务时，可以使用华为云联合全球知名证书服务商提供的证书管理服务。通过给Web网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输。
2-8-4	应定期审查密码学的网络安全要求。	华为云每年会对建立的密码算法应用及密钥管理安全相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对密码学的网络安全要求进行审查和更新。

5.2.9 备份与恢复管理

根据组织政策和程序以及相关法律法规，确保组织的数据和信息，包括信息系统和软件配置免受网络风险。

编号	具体控制要求	华为云的内部实践	客户的责任
2-9-1	应定义、记录和批准备份和恢复管理的网络安全要求。	华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。同时，华为云制定了数据备份规范，规范华为云管理节点数据备份格式、备份时间、备份内容和策略。此外，华为云还规范了业务恢复策略的制定，确保业务能在恢复时间目标内恢复到可接受水平。	客户应制定备份与恢复的安全管理策略，定义组织对信息、软件和系统备份的要求。
2-9-2	应实施备份和恢复管理的网络安全要求。	华为云提供高可用基础设施、冗余数据备份、可用区灾备等，还制定了业务连续性计划，并定期对其进行测试，以确保服务的高可用性，让云服务能够持续运行，保障客户的业务和数据安全。	客户应遵循已制定的备份管理机制，对关键业务数据、操作系统、应用软件进行备份。
2-9-3	备份和恢复管理的网络安全要求应至少包括以下内容：		
	2-9-3-1 涵盖关键技术和服务资产的备份范围和覆盖范围。	华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。华为云对于建立了节点数据备份机制，通过eBackup系统实现对节点数据的备份，且备份失败时自动通过邮件发送给备份管理员进行跟进。华为云支持在一个数据中心的多个节点内复制存放用户数据。单个节点一旦出现故障，用户数据不会丢失，系统可以做到自动检测和自愈。单个区域内不同可用区之间，通过高速光纤实现数据中心互联，满足跨可用区数据复制基本要求，用户可根据业务需求选择灾备复制服务。此外，像华为云提供的存储和数据库服务均具备高可靠保证，例如EVS云硬盘使用多副本的数据冗余保护机制，采用副本同步写、读修复等措施保证数据一致性，当检测到硬件故障能够自动后台修复，数据快	客户应明确关键技术和服务资产的备份范围，对关键业务数据、操作系统、应用软件进行备份。 如果客户需要对业务数据、软件和系统镜像进行备份，华为云提供了多种有不同侧重的产品和服务。例如，客户可以使用华为云提供的云备份(CBR - Cloud Backup and Recovery)服务对云内的云服务器、云硬盘、文件服务，云下文件、VMware虚拟化环

	<p>速自动重建，数据持久性可达 99.9999999%。；OBS 对象存储服务通过支持对象数据的高可靠性，并通过业务节点的高可靠性网络和节点的多冗余设计，使系统设计可用性达 99.995%，完全满足对象存储服务高可用的需求，通过提供对象数据多份冗余和保证多份对象的数据一致性自动修复技术，来提供对象数据的高可靠性，系统设计数据持久性高达 99.999999999%；RDS 关系型数据库服务采用热备架构，故障系统 1 分钟自动切换。每天自动备份数据，上传到 OBS 桶，备份文件保留 732 天，支持一键式恢复。</p>	<p>境进行备份，在发生病毒入侵、人为误删除、软硬件故障等导致数据不可用的场景前可将数据恢复到任意备份点。客户可使用云硬盘（EVS - Elastic Volume Service）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。华为云还为客户提供了镜像服务（IMS - Image Management Service），客户可使用该产品对云服务器的实例进行备份，当实例的软件环境出现故障时使用备份的镜像进行恢复。云服务器备份（CSBS - Cloud Server Backup Service）服务可同时为云服务器下多个云硬盘创建一致性在线备份，保护数据安全可靠，降低数据被非法篡改的风险。客户可以使用对象存储服务（OBS）的版本控制、云硬盘备份（VBS）、云服务器备份（CSBS）等功能，将云上的文档、硬盘、服务器进行备份。</p>
2-9-3-2 能够在网络安全事件后快速恢复数据和系统。	<p>华为云根据内部业务连续性管理体系的要求，为支撑云服务持续运行的关键业务制定了完善的恢复策略。恢复策略涵盖备用场地、设备、人员、信息系统、第三方等各个方面。同时，华为云数据中心集群的多地域（Region）和多可用区</p>	<p>客户应确保能够在发生网络安全事件后快速恢复数据和系统。</p> <p>客户可使用华为云提供的镜像服务 IMS，客户可通过</p>

		(AZ) 架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，可通过两地互为灾备中心，如一地出现故障，系统在遵循合规政策前提下自动将应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，在数据中心实现 N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。	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。
	2-9-3-3 定期测试备份的恢复效果。	华为云制定了业务连续性计划和灾难恢复计划，并定期对其进行测试。同时，华为云使用 eBackup 系统对备份数据进行循环冗余校验以确保备份数据的完整性和可用性，校验失败则无法成功进行备份。此外，华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。	客户需根据业务需求自行制定恢复测试计划，对备份的有效性进行测试。
2-9-4	应定期审查有关备份和恢复管理的网络安全要求。	华为云每年会对建立的备份与恢复和业务连续性相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对备份与恢复的网络安全要求进行审查和更新。

5.2.10 漏洞管理

确保及时发现和有效修复技术漏洞，以预防或尽量减少利用这些漏洞对该组织发起网络攻击的可能性。

编号	具体控制要求	华为云的内部实践	客户的责任
2-10-1	应定义、记录和批准技术漏洞管理的网络安全要求。	华为云建立了安全漏洞管理流程，规范了华为云系统安全漏洞的预警、评估、修复处理的闭环流程，并要求了定期安全关键安全补丁，降低漏洞风险，对漏洞定级、责任分配及漏洞处理要求进行规定。同时，华为云建立了专门的漏洞响应团队，及时评估并分析漏洞的原因、威胁程度及制定补救措施，评	客户应建立有效的漏洞管理机制，对所有技术资产进行漏洞识别和风险评估。

		评估补救方案的可行性和有效性。	
2-10-2	应实施技术漏洞管理的网络安全要求。	华为云相关人员遵循漏洞管理规范中定义的角色及职责，对漏洞进行定级、跟踪、修复和复核处理，持续跟踪确认风险得到消除或缓解。	客户应部署有效的工具以对技术基础设施进行监控，并定期对关键系统的网络组件进行脆弱性评估。
2-10-3	技术漏洞管理的网络安全要求应至少包括以下内容：		
	2-10-3-1 定期漏洞评估。	华为云建立了漏洞定期扫描机制，每月对报告范围内的产品执行漏洞扫描并由漏洞扫描团队负责对扫描结果进行跟踪处理。同时，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。华为云针对会影响客户服务的漏洞，华为云会发布漏洞公告，其中包括漏洞详情、漏洞原理分析、漏洞影响范围、漏洞防范措施及漏洞解决方法等内容。	客户根据漏洞扫描流程，以组织定义的频率对其信息系统进行漏洞扫描。华为云会第一时间针对紧急爆发的通用漏洞 CVE 进行分析并更新规则，提供快速、专业的 CVE 漏洞扫描。同时，客户可使用华为云的企业主机安全（Host Security Service，简称 HSS），检测 Windows/Linux 操作系统与 SSH、OpenSSL、Apache、Mysql 等软件存在的漏洞，并给出修复建议。此外，华为云可为客户提供容器安全服务（CGS - Container Guard Service）能够扫描镜像中的漏洞与配置信息，发现镜像中的漏洞并给出修复建议，帮助企业解决传统安全软件无法感知容器环境的问题。
	2-10-3-2 基于关键级别的漏洞分类。	华为云已建立起从漏洞感知到现网修复的端到端漏洞响应工单系统，基于业界最佳实践 CVSS（Common Vulnerability Scoring System）对漏	客户应分析漏洞对关键信息资产的影响，并根据其重要性确定风险等级

		洞进行严重级别的评估，并结合漏洞在华为云中被利用的风险评估结果决定处理优先等级，制定并落实漏洞修复方案或规避措施。	和修复优先级。
2-10-3-3 基于分类和相关风险级别的漏洞修复。	华为云已建立起从漏洞感知到现网修复的端到端漏洞响应工单系统，自动根据漏洞的严重程度确定处理优先级，从而明确对应的漏洞修复 SLA 要求。对于重大安全漏洞，安全运维团队可通过自研工具，对现网进行扫描，实现分钟级的受影响服务和模块的范围界定；同时安全运维团队会根据现网情况，采取必要的漏洞缓解措施，例如限制端口访问、实施 WAF 漏洞规则等方式对受影响的服务进行防护或隔离，以降低漏洞被利用的风险。对于需要通过版本、补丁修复的漏洞，通过灰度发布或蓝绿部署等方式尽量减少对租户业务造成影响。同时，华为云还持续更新操作系统及容器镜像，通过镜像和容器的滚动升级完成系统漏洞修复，不会对租户业务造成影响。	客户应根据漏洞的重要程度，定义并分配时间范围，在定义的响应时间内完成漏洞修复。	
2-10-3-4 安全补丁管理。	华为云建立安全补丁管理的流程，保证安全补丁在 IT 安全标准规定的期限内完成安装。同时，华为云制定了漏洞管理机制，确保对云平台及云服务安全漏洞及时的应急响应，不断优化云平台及云产品默认安全配置、及时在规定的期限内应用修补措施或补丁、补丁装载前置与研发阶段和灵活简化安全补丁部署周期等。	客户应建立有效的补丁和漏洞管理机制，对所有技术资产进行漏洞识别和风险评估，对关键补丁进行测试，制定补丁更新周期以及补丁修复的工作流程。 华为云镜像服务（IMS）简单方便的镜像自助管理功能。客户可通过服务控制台或 API 对自己的镜像进行管理。华为云负责公共镜像的定期更新与维护向用户提供安装安全补丁的公共镜像和相关安全加固和补丁信息以便用户在部署测试、故障排除等	

			运维活动时参考。
	2-10-3-5 订阅授权和受信任的网络安全资源，以获取有关技术漏洞的最新信息和通知。	华为云 PSIRT 会主动监控业界知名漏洞库、安全论坛、邮件列表、安全会议等渠道，以保证第一时间感知到包括云在内的华为相关漏洞信息。通过建立包括云业务在内的所有产品和解决方案的公司级漏洞库，以保证有效记录、追踪和闭环每个漏洞。	客户应从信息共享平台收集和分析网络威胁情报，订阅授权和受信任的网络安全资源，以获取有关技术漏洞的最新信息和通知。
2-10-4	应定期审查技术漏洞管理的网络安全要求。	华为云每年会对建立的漏洞管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对漏洞管理的网络安全要求进行审查和更新。

5.2.11 渗透测试

通过模拟网络攻击评估该组织的网络安全防御能力的效率，以发现技术基础设施中可能导致网络入侵的未知弱点。

编号	具体控制要求	华为云的内部实践	客户的责任
2-11-1	应定义、记录和批准渗透测试活动的网络安全要求。	华为云建立了渗透测试与漏洞扫描管理规定，明确了华为云平台开展渗透测试时应遵循的安全要求，规范渗透测试行为，确保渗透测试活动合规与受控。	客户应制定渗透测试管理规范，规范渗透测试行为。
2-11-2	应实施渗透测试流程的网络安全要求。	华为云相关人员遵循渗透测试与漏洞扫描管理规范中定义的实施流程，制定并实施具体的渗透测试活动，发现的漏洞和风险需与相关业务人员进行评估并形成正式的渗透测试报告，并向网络安全与隐私保护办公室的汇报。	客户应遵循已制定的渗透测试管理规范，根据自身业务需求对系统和网络进行渗透测试。华为云还可以提供渗透测试的安全专家服务。
2-11-3	渗透测试流程中的网络安全要求应至少包括以下内容：		
	2-11-3-1 渗透测试范围应涵盖面向 Internet 的服务及其技术组件，包括基础设施、网站、Web	华为云每半年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，渗透测试报告及跟进情况会通过内部审计以及外部认证机	客户应明确渗透测试的范围，覆盖面向 Internet 的服务机器技术组件。

	应用程序、移动 应用程序、电子 邮件和远程访 问。	构核查。	
	2-11-3-2 定期进 行渗透测试。	华为云每半年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，渗透测试报告及跟进情 况会通过内部审计以及外部认证机 构核查。	客户应定期对网络 基础和系统进行渗 透测试。
2-11- 4	应定期审查渗 透测试过程中的网 络安全要求。	华为云每年会对建立的渗透测试与 漏洞扫描管理相关规范和策略流程 进行审阅和更新，同时华为云网络 安全与隐私办公室定期对策略的执 行情况进行定期的审视，确保安全 治理的策略、标准、规范和具体措 施在各业务领域的流程落地。	客户应根据计划的 频率定期对渗透测 试的网络安全要求 进行审查和更新。

5.2.12 网络安全事件日志与监控管理

确保及时收集、分析和监控网络安全事件，以便及早发现潜在的网络攻击，以防止或尽量减少对组织的负面影响。

编号	具体控制要求	华为云的内部实践	客户的责任
2-12- 1	应定义、记录和 批准对事件日志 和监控管理的网 络安全要求。	华为云建立了安全日志管理规范， 规范了华为云应用系统、服务、网 络设备安全日志的管理，确保网络 安全事件的回溯。	客户应制定事件日 志与监控的安全管 理策略，及时发现 系统中可能存在的 网络入侵的安全风 险。
2-12- 2	应实施对事件日 志和监控管理的 网络安全要求。	华为云建立了集中、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，以确保支撑网络安全事件 回溯。	客户应遵循已建立 的事件日志与监控 的安全管理策略， 确保可追溯所有活 动的操作，日志的 保留期限还应满足 法规要求。
2-12- 3	事件日志和监控管理的网络安全要求应至少包括以下内容：		
	2-12-3-1 开启关 键信息资产上的 网络安全事件日 志。	华为云建立了统一的日志分析平 台，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	客户应收集所有关 键信息资产上的网 络安全事件日志。 华为云提供的云日

		威胁检测告警日志。 华为云的统一日志分析平台，对 SVN、堡垒机、主机、WAF、HSS 等服务的安全日志进行收集并建立日志监控自动告警机制。运维平台作为华为云进行运维管理的入口，开启了操作日志记录的功能，操作日志无法被人为修改，且至少保留了 6 个月的日志记录，包括登录 IP、登录方式及登陆时间等。	志服务（LTS - Log Tank Service）提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。 客户应记录远程访问和特权用户账户的操作日志。 华为云的云审计服务（CTS）为用户提供云服务资源的操作记录，供用户查询、审计和回溯使用。记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的 API 执行的操作，以及华为云系统内部触发的操作。
	2-12-3-3 识别网络安全事件日志收集所需的技术（例如，SIEM）。	华为云建立了集中、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，以确保支撑网络安全事件回溯。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM - Security Information and Event Management）系统如 ArcSight、Splunk 对接。	客户应使用必要的技术对网络安全事件日志进行收集和分析。
	2-12-3-4 持续监控网络安全事件。	对于集中存储安全日志的日志分析平台，系统管理员会定期例行对采集状态、存储状态进行检查，保证安全日志的可用性。华为云日志分析平台对产品相关运维系统、服务器及网络设备的安全日志进行了收录，同时在平台内预设了异常操作	客户应建立监控平台对各个系统的安全日志进行持续监控和必要分析，及时检测和响应安全事态和事件。 华为云提供的云日

		规则，用于识别用户进行异常操作的情形，自动生成告警信息并推送至相关安全部门进行后续跟进处理，异常告警按照服务等级协议要求及时处理并通过事件分析处理平台进行实时大屏监控与记录。	志服务（Log Tank Service，简称 LTS）提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。结合云监控服务（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。客户可以对用户登录日志进行实时监控，当遇到恶意登陆行为可触发告警并拒绝该 IP 地址的请求。
	2-12-3-5 网络安全事件日志的保留期（必须至少为 12 个月）。	日志分析系统有强大的数据保存及查询能力，确保所有日志保存时间为 12 个月。	客户应确保网络安全事件日志的保留其必须为 12 个月。 华为云的云审计服务（Cloud Trace Service，简称 CTS）可以实时、系统地记录用户通过云账户登录管理控制台执行的操作。客户可根据企业对日志保留期限的要求购买不同规格的对象存储服务服务（Object Storage Service，简称 OBS）以实现日志的备份。
2-12-4	应定期审查有关事件日志和监控管理的网络安全要求。	华为云每年会对建立的安全日志管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业	客户应根据计划的频率定期对事件日志与监控管理的网络安全要求进行审查和更新。

		务领域的流程落地。	
--	--	-----------	--

5.2.13 网络安全事件与威胁管理

确保及时识别、检测、有效管理和处理网络安全事件和威胁，以防止或尽量减少对组织运营的负面影响。

编号	具体控制要求	华为云的内部实践	客户的责任
2-13-1	应定义、记录和批准对网络安全事件和威胁管理的要求。	华为云内部制定了安全事件管理机制，规范了华为云安全事件响应操作，明确华为云安全事件定级及通报机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。	客户应制定网络安全事件管理策略，建立安全事件上报和决策流程，并采取适当应对计划和沟通策略。
2-13-2	应实施对网络安全事件和威胁管理的要求。	华为云建立了统一的事件分析处理平台实现对安全事件的统一收集，并针对收集上来的安全事件进行统一的跟踪管理，确保安全事件得以被及时处理及修复。	客户应遵循已制定的网络安全事件管理策略，对各个系统的安全日志进行持续监控和必要分析，及时检测和响应安全事态和事件。
2-13-3	网络安全事件和威胁管理的要求应至少包括以下内容：		
	2-13-3-1 网络安全事件响应计划和升级程序。	华为云建立了事件处理流程，在出现安全事件时遵循华为云事件响应流程（识别、评估、决策和执行应急响应处理）。同时华为云规范了安全事件的升降原则，在溯源分析事件时若新风险被识别，则新增安全事件的定级需要衡量统一事件累计的结果，重新对其进行定级响应。	客户应制定网络安全事件响应计划，并建立安全事件上报升级流程。
	2-13-3-2 网络安全事件分类。	华为云内部制定了完善的事件管理流程，根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的处理时限。在事件发生后，华为云将根据事件的优先级，在规定的时限内对事件进行响应和解决，最大化降低事件对客户造成的影响。	客户应根据事件的影响程度和范围的不同对网络安全事件进行分类。
	2-13-3-3 向 NCA	华为云针对安全事件带来的影响及	当发生网络安全事

	报告的网络安全事件。	处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。为配合客户满足网络安全事件上报NCA的要求，华为云设置7*24的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。	件时，客户应按照本规定的要求向NCA上报。
2-13-3-4 与 NCA 共享事件通知、威胁情报、违规指标和报告。	华为云针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。为配合客户满足网络安全事件上报NCA的要求，华为云设置7*24的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。	客户应按照本规定的要求与 NCA 共享事件通知、威胁情报、违规指标。	
2-13-3-5 收集和处理威胁情报源。	华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。支持众多威胁分析模型和算法，结合威胁情报和安全咨询，精准识别攻击，并且该系统实时评估华为云安全状态，分析潜在风险，	客户应多渠道收集和分析网络威胁情报。 态势感知（SA - Situation Awareness）是华为云为客户提供的安全管理与态势分	

		并结合威胁情报进行预警，做好预防工作。	析平台。能够检测出包括 DDoS 攻击、暴力破解、Web 攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等多种云上安全风险。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为客户呈现出全局安全攻击态势，帮助客户识别、收集及获取信息安全事件相关证据并通过分析事件以减少事件在未来发生的可能性和影响。同时态势感知可以关联 DDoS 高防、企业主机安全服务、Web 应用防火墙和数据库安全服务等，集中呈现安全防护状态。
2-13-4	应定期审查对网络安全事件和威胁管理的要求。	华为云每年会对建立的安全事件管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对网络安全事件与威胁的安全要求进行审查和更新。

5.2.14 物理安全

确保信息和技术资产免受未经授权的物理访问、丢失、盗窃和损坏。

编号	具体控制要求	华为云的内部实践
2-14-1	应定义、记录和批准信息和技术资产物理保护的网络安全要求。	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。华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介

		质等)的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。
2-14-2	应实施对信息和技术资产的物理保护的网络安全要求。	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。华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施(包括门禁、安全岗、摄像监控等)及设备出入控制(包括拍照摄影设备、存储介质等)的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。
2-14-3	信息和技术资产物理保护的网络安全要求应至少包括以下内容： 2-14-3-1 授权访问组织内的敏感区域(如数据中心、灾难恢复中心、敏感信息处理设施、安全监控中心、网络机柜)。	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。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。
	2-14-3-2 设施进出记录和闭路电视监控。	华为云制定了存储介质及设备进出机房管理规定，要求存储介质及设备进出机房前需进行登记并得到授权。物理存储介质进出机房时均会进行数据防泄漏管理，并对数据擦除、报废清退流程进行规定，减少可能存在的数据泄露损失。
	2-14-3-3 保护设施进出和监视记录。	华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施(包括门禁、安全岗、摄像监控等)及设备出入控制(包括拍照摄影设备、存储介质等)的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。
	2-14-3-4 安全销毁和重新使用保存机密信息的物理资产(包括文件和存储介质)。	华为云使用包含存储介质的设备由专人管理，使用完毕后由专人对其进行格式化处理。存储公司保密信息的存储介质报废时由专人确保其上存储的信息均被清除且不可恢复，处理方式包括消磁、物理销毁或低级格式化。
	2-14-3-5 组织设施内外的设备和设备的安全。	华为云制定了机要设备与介质管理相关规定，对设备的安置、保护、进出等均做出要求并制定操作流程。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。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。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，确保非授权人员不可访问数据中心。
2-14-4	应定期审查对信息和技术资产的	华为云每年会对建立的物理与环境安全相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公

	物理保护的网络安全要求。	室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。
--	--------------	---

5.2.15 Web 应用安全

确保外部 Web 应用程序免受网络风险。

编号	具体控制要求	华为云的内部实践	客户的责任
2-15-1	应定义、记录和批准外部 Web 应用程序的网络安全要求。	华为云各服务可通过公开的 API 进行配置管理，华为云明确了 API 应用安全管理要求，对身份认证及鉴权、传输保护、边界防护及流量控制的有效保护进行了定义。	客户应定义外部 Web 应用程序的网络安全要求。
2-15-2	应实施外部 Web 应用程序的网络安全要求。	华为云对在公共网络上提供的应用服务采用多重机制和措施进行重点保护，包括使用 IAM 进行访问控制，对用户进行身份认证和鉴权；API 调用使用 TLS 加密以保证传输的机密性；结合 Anti-DDoS、入侵防御系统（IPS）和 Web 应用防火墙（WAF）等多层高级边界防护机制针对不同的威胁和攻击进行有效防范；对用户调用 API 的频率的适当流量控制，确保基于 API 的访问的高可用性和连续性。	客户应根据已制定的外部 Web 应用程序的安全要求，实施适用的措施确保外部 Web 应用程序免受网络风险。
2-15-3	外部 Web 应用程序的网络安全要求应至少包括以下内容：		
	2-15-3-1 Web 应用防火墙的使用。	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、XSS、CSRF 等面向应用软件的攻击。	客户应部署 Web 应用防火墙。 客户可通过部署 Web 应用防火墙（WAF -Web Application Firewall）对网站业务流量进行多维度检测和防护。Web 应用防火墙可结合深度机器学习智能识别恶意请求特征和防御未知威胁，通过对 HTTP(S)请求进行检测，识别并阻断 SQL 注入、跨站

		脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，全面避免网站被黑客恶意攻击和入侵，保护 Web 服务安全稳定。
2-15-3-2 采用多层架构原则。	华为云参照业界实践并结合自身经验沉淀及业务特性从三层技术架构设计 Web 应用程序，包括基础层（application layer）、平台层（platform layer）、应用层（foundation layer），实现应用的安全设计与维护，确保高内聚，低耦合。此外，华为云制定了 web 应用开发规范，结合多维度的安全开发原则，实现深度防御的目的。	客户应采用多层架构原则。
2-15-3-3 使用安全协议（例如 HTTPS）。	华为云提供的公共 API 接口均强制要求使用超文本传输安全协议（HTTPS）进行通信，且 API 调用需使用 TLS 加密以保证传输的机密性。目前 API 网关所有对外网开放的 API 均使用 TLS 1.2 版本加密协议，并且支持 PFS（Perfect Forward Secrecy）安全特性。	客户应使用安全协议（如 HTTPS）进行通信。
2-15-3-4 为用户阐明安全使用政策。	华为云作为云服务提供商，定义了华为云安全责任共担模型，明确了华为云与客户双方的安全责任边界，和各自应承担的安全责任。华为云的各云产品均会为客户提供包括帮助文档、使用手册、安全实施指南等，其中会包含安全使用的政策。	客户开发的外部 Web 应用程序应为其用户提供帮助文档、使用手册等，说明安全使用政策。
2-15-3-5 用户访问的多因素认证。	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。华为云的统一身份认证服务（IAM）为客户提供适合企业级组织结构的用户账号管	客户开发的外部 Web 应用程序应为其用户提供多因素的访问认证。 客户可使用华为云统一身份认证服务，默认启用多因

		理、身份认证和细粒度的云上资源访问控制。IAM 提供多因素认证（MFA）功能，提高账号登录和重要操作的安全性。	子认证，保证用户账号安全。
2-15-4	应定期审查外部 web 应用程序的网络安全要求。	华为云每年会对建立的 API 应用安全相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对外部 Web 应用程序的网络安全要求进行审查和更新。

5.3 网络安全弹性

“网络安全弹性”为客户实施有效的业务连续性管理提供了实施指引，涵盖业务连续性计划的开发、应急响应计划及灾难恢复计划的实施等方面。相关控制要求及华为云的实践方式如下：

5.3.1 业务连续性管理 (BCM) 的网络安全弹性方面

确保将网络安全弹性要求纳入组织的业务连续性管理，并纠正且最大限度地减少网络安全事件造成的灾难对系统、信息处理设施和关键电子服务的影响。

编号	具体控制要求	华为云的应答	客户的责任
3-1-1	应定义、记录和批准业务连续性管理的网络安全要求。	华为云制定了业务连续性管理规定，以规范业务连续性相关管理框架、目的和范围、管理目标、角色和职责等内容。华为云已经通过 ISO22301 业务连续性管理体系标准的认证，并制定了业务连续性计划，其中包含了自然灾害、事故灾害、信息技术风险等突发事件的应对策略与应对流程。	客户应建立业务连续性管理机制，明确有关服务的恢复目标及最小恢复策略。
3-1-2	应实施业务连续性管理的网络安全要求。	华为云已经通过 ISO22301 业务连续性管理体系标准的认证。华为云每年执行一次业务影响分析和风险评估，识别关键活动及依赖、评估风险等级，并对识别出的可造成云服务资源中断的威胁制定应对策略，形成业务连续性计划。	客户应根据制定的业务连续性管理机制，定期开展业务影响分析，识别关键业务，确定关键业务的恢复时间目标，为此类活动分配足够的资源，符合客户自身业务连续性和法规要求。

2-13-3	业务连续性管理的网络安全要求应至少包括以下内容：		
	3-1-3-1 确保网络安全系统和程序的连续性。	华为云每年执行一次业务影响分析和风险评估，识别关键活动及依赖、评估风险等级，并对识别出的可造成云服务资源中断的威胁制定应对策略，形成业务连续性计划。同时，华为云在业务连续性管理体系范围内的云服务均采用单地域多数据中心的冗余机制，以确保云服务的业务连续性。	客户应定期开展业务影响分析，识别关键业务，确定关键业务的恢复时间目标，针对业务影响分析的结果制定恢复策略，以确保网络安全系统和程序的连续性。 客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。
	3-1-3-2 为可能影响业务连续性的网络安全事件制定响应计划。	华为云针对各产品可能涉及的不同突发场景，规范了应急响应工作流程，形成应急响应预案。同时，华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。	客户应按照业务影响分析制定业务连续性计划及灾难恢复计划，防范和减少突发事件导致的业务中断。
	3-1-3-3 制定灾难恢复计划。	华为云还制定了灾难恢复计划，并定期对其进行测试。例如，将一个地理位置或区域的云平台基础架构和云服务处于离线状态，模拟一个	客户应按照业务影响分析制定业务连续性计划及灾难恢复计划，防范和减

		<p>灾难，然后按照灾难恢复计划进行系统处理和转移，以验证故障位置的业务及营运功能，测试结果将被注释并记录归档，用以持续改进该计划。</p>	<p>少突发事件导致的业务中断。客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。</p> <p>此外，为满足组织在灾难发生时对信息安全及信息安全管理连续性的要求，华为云向客户提供存储容灾服务（SDRS - Storage Disaster Recovery Service）为弹性云服务器、云硬盘和专属分布式存储（DSS - Dedicated Distributed Storage Service）等服务提供容灾与灾难恢复。存储容灾服务通过存储复制、数据冗余和缓存加速等多项技术，提供给用户高级别的数据可靠性以及业务</p>
--	--	--	--

			连续性。存储容灾服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到容灾站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。
3-1-4	应定期审查业务连续性管理的网络安全要求。	华为云每年会对建立的业务连续性管理体系进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对业务连续性管理的网络安全要求进行审查和更新。

5.4 第三方与云计算网络安全

“第三方与云计算网络安全”为客户实施业务外包提供了指引。对客户的控制要求覆盖服务供应商能力、合同和协议、客户数据机密性、云服务的使用等领域。相关控制要求及华为云的实践方式如下：

5.4.1 第三方网络安全

根据组织政策和程序以及相关法律法规，确保资产免受与第三方相关的网络安全风险，包括外包和托管服务。

编号	具体控制要求	华为云的内部实践	客户的责任
4-1-1	应确定、记录和批准与第三方签订的合同和协议的网络安全要求。	华为云提供了线上的《华为云用户协议》以及华为云《云服务等级协议》，其中规定了所提供的服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。 在华为云内部，华为云建立了正式的采购审核流程，在供应商入场前，华为云要求须同供应商签署合同、服务协议及保密协议。合同与服务协议中明确了双方的责任和义务、供应商应满足的网络安全要	客户应在与第三方签订的合同和协议中明确网络安全要求，降低第三方访问组织资产的相关风险。

		求、服务内容及服务水平等要求，同时通过保密协议对违反保密性的条款进行了约束。华为云法务部门每年会对采购保密协议进行审阅及更新，以确保采购保密协议可以持续满足业务对供应商的管理要求。	
4-1-2	与第三方签订的合同和协议（例如，服务水平协议 (SLA)）的网络安全要求——如果受到影响，可能会影响组织的数据或服务——应至少包括以下内容：		
	4-1-2-1 保密条款和第三方在服务结束时安全删除组织的数据。	在客户确认删除数据后，华为云会对指定的数据及其所有副本进行全面的清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。 在华为云内部，华为云在引入供应商时会与其签署保密及服务水平协议，协议中包含对于供应商的安全和隐私数据处理的要求。同时，华为云制定了供应商个人信息保护政策，明确对各供应商在隐私及数据保护方面须遵循的管理要求进行了定义。	客户应在与第三方签订的合同或协议中明确第三方在服务结束时使用安全措施删除组织的数据。 在服务协议终止时，客户可通过华为云提供的云数据迁移服务 (CDM)，将内容数据从华为云中迁移出去，如迁移至本地数据中心。
	4-1-2-2 发生网络安全事件时的沟通程序。	针对影响客户的安全事件，华为云建立了完善的事件通告机制。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。 在华为云内部，华为云与供应商签订的合同和协议中，会约定发生网络安全事件时的沟通和响应流程。	客户应在与第三方签订的合同或协议中明确发生网络安全事件时的沟通程序。
	4-1-2-3 第三方遵守相关组织政策和程序、法律法规的要求。	华为云恪守“不碰数据”底线，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令，并严	客户应在与第三方签订的合同或协议中明确第三方须遵守组织政策和程序、法律法规的要

		<p>格遵守《ECC》所述的网络安全原则。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。</p> <p>在华为云内部，供应商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。针对华为云的供应商，华为云会定期对其服务的安全合规性进行评估，对其可以提供的用户个人信息安全性保护能力进行评估。</p>	求。
4-1-3	与 IT 外包和托管服务第三方签订的合同和协议的网络安全要求必须至少包括以下内容：	<p>4-1-3-1 进行网络安全风险评估，以确保在签订合同和协议之前或在相关法规要求发生变化时缓解风险控制措施的可用性。</p>	<p>华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。</p> <p>在华为云内部，华为云已建立供应商选择和监督体系，并规范了研发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。</p>
	4-1-3-2 用于监控和运营的网络安全托管服务中心应完全存在于沙特阿拉伯王国境内。	<p>华为云会将用于监控和运营的网络安全服务中心部署在沙特阿拉伯王国境内。此外，华为云提供云监控服务（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。CES 提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。CES 的监控对象是基础设施的资源使用数据，不监控或触碰租户数据。</p>	客户应确保用于监控和运营的网络安全托管服务中心位于沙特阿拉伯王国境内。
4-1-4	应定期审查与第三方签订的合同和协议的网络安全要求。	华为云法务部门每年会对采购保密协议进行审阅及更新，以确保采购保密协议可以持续满足业务对供应商的管理要求。	客户应根据计划的频率定期审查和更新与第三方签订的合同和协议的网络安全要求。

5.4.2 云计算与托管网络安全

根据组织政策和程序以及相关法律法规，确保对网络风险进行适当和有效的补救，并实施与托管和云计算相关的网络安全要求。这也是为了确保对托管在云上或由第三方处理/管理的组织的信息和技术资产的保护。

编号	具体控制要求	华为云的内部实践	客户的责任
4-1-1	应定义、记录和批准与使用托管和云计算服务相关的网络安全要求。	华为云作为云服务提供商，确保各项目云技术的安全开发、配置和部署以及所提供云服务的运维运营安全。华为云参照 ISO27001、ISO27017、ISO27018、SOC、CSA STAR 的要求构建了信息安全管理体系，制定了华为云整体的信息安全策略，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标。	客户应建立使用托管和云计算服务相关的网络安全要求，确保托管在云上的组织的信息和技术资产的安全。
4-1-2	应实施与使用托管和云计算服务相关的网络安全要求。	华为云遵循已建立的信息管理体系，包括资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性得等多个安全领域，全方位保护客户系统和数据的保密性、完整性和可用性。华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应遵循已建立的使用托管和云计算服务的网络安全要求。
	根据相关和适用的法律法规，除主域(1)、(2)、(3)和子域(4-1)适用 ECC 控制外，与使用托管和云计算服务应至少包括以下内容：		
4-2-3	4-2-3-1 在云上托管或托管服务之前对数据进行分类，并在服务完成后返回数据（以可用格式）。	华为云提供的云数据迁移服务（CDM），支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓库、文件等，并且支持在多个环境之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。	客户在使用云服务之前，需要对其数据进行分类，并进行风险分析，再根据风险分析结果，明确防护数据的存储位置、存储服务和安全防护措施。 在服务协议终止时，客户可通过华为云提供的云数据迁移服务（CDM），将内容数据从华为云中迁移出去，如迁移至

			本地数据中心。
	4-2-3-2 将组织的环境（特别是虚拟服务器）与云服务提供商托管的其他环境分开。	虚拟私有云服务（VPC – Virtual Private Cloud）为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化用户的网络部署。华为云对云端数据的隔离是通过虚拟私有云（VPC – Virtual Private Cloud）实施的，VPC 采用网络隔离技术，实现不同租户间三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置：一方面，结合 VPN 或云专线，将 VPC 与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用 VPC 的 ACL、安全组功能，按需配置安全与访问规则，满足租户更细颗粒度的网络隔离需要。	客户应将组织环境与云服务商托管的其他环境分开。
	4-2-3-3 组织的信息托管和存储应在沙特阿拉伯王国境内。	华为云会将组织的信息托管和存储部署在沙特阿拉伯王国境内。	客户应确保组织的信息托管和存储位于沙特阿拉伯王国境内。
4-2-4	应定期审查与使用托管和云计算服务相关的网络安全要求。	华为云作为云服务提供商，每年会对建立的信息安全管理进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对使用托管和云计算有关的网络安全要求进行审查和更新。

6 华为云如何符合《CCC 云计算控制》的要求

《CCC 云计算控制》是作为 ECC 的扩展而制定的，通过从云服务提供商（CSPs）和云服务租户（CSTs）的角度，阐述云计算服务需实现的网络安全目标，为客户实施云计算服务提供了网络安全要求。其中涵盖了网络安全治理、网络安全防御、网络安全弹性、第三方网络安全四大领域。

以下内容将总结 CCC 中云服务提供商相关的控制相关，并详细阐述了华为云作为客户的云服务供应商时，会如何帮助客户满足这些控制要求。

6.1 网络安全治理

“网络安全治理”要求云服务提供商建立适当的网络安全管理机制，涵盖网络安全战略、策略与程序、项目管理、风险管理等网络安全治理领域。相关控制要求及华为云的实践方式如下：

6.1.1 网络安全角色与责任

确保为参与实施云网络安全控制的所有各方定义角色和责任，包括 CSP 和 CST 负责人或其代表的角色和责任，在本控制中称为“授权官员/授权人员”。

编号	具体控制要求	华为云的践行方式
1-1-P-1	除 ECC 控制 1-4-1 外，授权官员还应识别、记录和批准： 1-1-P-1-1 云服务所有利益相关者的网络安全角色和 RACI 分配，包括授权官员的角色和职责。	在华为公司层面，全球网络安全与用户隐私保护团队 GSPC 作为最高网络安全管理机构，决策和批准公司总体网络安全战略。GSPO 及其办公室负责制定和执行华为端到端网络安全保障体系。华为云网络安全与用户隐私保护团队负责制定华为云安全策略，并定期对策略的执行情况进行定期审视，确保安全治理的策略、规范和具体措施在各业务领域的流程落地，实现端到端的安全治理。同时，华为云在各产品、服务的业务团队中明确规定了所有员工对应角色的网络安全

		责任，华为云设置专门负责安全及隐私保护的角色承担一定的安全管理职责。网络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。沙特网络安全与隐私保护官遵循公司最高层面的网络安全战略，并在沙特执行落地。
--	--	--

6.1.2 网络安全风险管理

确保以系统性方法管理网络安全风险，以根据组织政策和程序以及相关法律法规保护 CSP 和 CST 的信息和技术资产。

编号	具体控制要求	华为云的践行方式
1-2-P-1	ECC 子域 1-5 中提到的网络安全风险管理方法至少还应包括 CSP:	
	1-2-P-1-1 定义云服务可接受的风险级别，如果与 CST 相关，则向 CST 说明。	在开展风险评估中，相应领域的业务专家全程参与，以确保准确评估风险对业务的影响和风险的级别；网络安全与隐私保护专家提供类似场景的风险评估结果、发生过的安全事件和安全隐私合规要求等信息，协助业务专家充分识别风险。根据风险对机密性、完整性、可用性及合规性的影响，以及发生的可能性对整体风险进行定级（低、中、高风险）。完成风险定级后，风险管理员将发送风险管理邮件，告知风险详情，风险等级、风险处置 SLA 等，并告知风险接口人及安全和业务的相关人员。如涉及到云租户的安全性、可用性等风险，则会及时将会对云租户造成的影响进行公告。
	1-2-P-1-2 考虑网络安全风险管理方法中的数据和信息分类。	华为云遵循已制定的网络安全风险评估方法，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断。同时风险评估涵盖数据安全的各方面，包括数据保护和分类、数据留存和传输位置、数据保存时间对法律法规的符合等。
	1-2-P-1-3 制定云服务网络安全风险登记表，并根据风险定期监测。	风险管理员认识各业务场景中所涉及的风险，将风险及时录入风险管理平台，包括风险描述、所属领域、风险等级、风险来源等形成风险清单，并利用风险管理平台对风险进行自动跟踪与监控。

6.1.3 网络安全标准、法律和法规合规

确保 CSP 和 CST 的网络安全计划符合相关法律法规。

编号	具体控制要求	华为云的践行方式
----	--------	----------

1-3-P-1	<p>除了 ECC 控制 1-7-1 外, CSP 的立法和法规规定至少应包括以下要求:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding: 5px;">1-3-P-1-1 持续性遵守 KSA 所有的法律、法规、指示、决定, 关于网络安全的监管框架和控制, 以及授权。</td><td style="width: 70%; padding: 5px;">华为云在其网络安全策略中明确合规流程, 定期识别和记录合规要求。同时, 华为云设立了专岗同外部各方保持积极的联系, 以追踪法律、法规的相关要求变化。当识别到与华为云服务相关的法律、法规, 华为云将及时调整内部安全要求和安全控制水平, 跟进对法律、法规要求的符合性。此外, 华为云针对 KSA 网络安全相关的法律法规、标准及框架进行了识别并梳理形成白皮书, 以证明其合规性。</td></tr> </table>		1-3-P-1-1 持续性遵守 KSA 所有的法律、法规、指示、决定, 关于网络安全的监管框架和控制, 以及授权。	华为云在其网络安全策略中明确合规流程, 定期识别和记录合规要求。同时, 华为云设立了专岗同外部各方保持积极的联系, 以追踪法律、法规的相关要求变化。当识别到与华为云服务相关的法律、法规, 华为云将及时调整内部安全要求和安全控制水平, 跟进对法律、法规要求的符合性。此外, 华为云针对 KSA 网络安全相关的法律法规、标准及框架进行了识别并梳理形成白皮书, 以证明其合规性。
1-3-P-1-1 持续性遵守 KSA 所有的法律、法规、指示、决定, 关于网络安全的监管框架和控制, 以及授权。	华为云在其网络安全策略中明确合规流程, 定期识别和记录合规要求。同时, 华为云设立了专岗同外部各方保持积极的联系, 以追踪法律、法规的相关要求变化。当识别到与华为云服务相关的法律、法规, 华为云将及时调整内部安全要求和安全控制水平, 跟进对法律、法规要求的符合性。此外, 华为云针对 KSA 网络安全相关的法律法规、标准及框架进行了识别并梳理形成白皮书, 以证明其合规性。			

6.1.4 人力资源网络安全

根据组织政策和程序以及相关法律法规, 确保与人员 (员工和承包商) 相关的网络安全风险在雇佣前、雇佣期间和终止/离职后均得到有效管理。

编 号	具体控制要求	华为云的践行方式
1-4-P-1	除了 ECC 控制中 1-9-3 和 1-9-4 中的子控制之外, 在人员与 CSP 建立专业关系之前及建立关系期间, 应至少满足以下要求:	
	1-4-P-1-1 网络安全职能在 KSA 内 CSP 数据中心的位置必须由合格且合适的沙特国民担任。	华为云会任命合格且合适的沙特国民担任网络安全职能在 KSA 内 CSP 数据中心的位置。
	1-4-P-1-2 定期筛选或审查在 KSA 内工作且有权访问云技术堆栈的人员的候选人。	华为云遵循华为公司的整体人力资源管理框架建立了人员信息安全管理规定, 明确了华为云各类员工分层分级的信息安全管理要求, 对内外部员工关于招聘、培训、稽核和奖罚等方面管理进行了规范, 明确了员工应遵循的华为云网络安全职责。在任用华为云正式员工或外包人员时, 均进行严格的背景审查, 确保员工背景和资历适合华为云安全业务要求, 其中针对可访问云技术堆栈的运维工程师等重点关键岗位实施专项管理, 包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。
	1-4-P-1-3 已签署并批准网络安全政策是访问云技术堆栈先决条件。	员工与公司签署的聘用协议中包含保密条款, 其中明确规定员工的网络安全责任, 以确保在入职前对应遵循的保密条款进行确认。华为云规定员工离职时需签署离职保密承诺书, 确认其应持续承担的信息安全责任及职责。华为云将网络安全纳入华为员工商业行为准则, 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。此外, 运维人员需通过工单系统或书面获得客户授权后, 使用指定工具才允许接入客户环境, 严禁进行超出客户授权范围的任何操作及

		禁止类的高危操作。
1-4-P-2	除了 ECC 控制 1-9-5 中的子控制之外，还应至少满足以下要求以终止/完成人力资源与 CSP 的专业关系：	
	1-4-P-2-1 保证组织拥有的资产（尤其是那些有安全风险的资产）在终止时得到核算和归还。	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，此外华为云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。华为云规定员工离职时需签署离职保密承诺书，确认其应持续承担的信息安全责任及职责。

6.1.5 网络安全变更管理

根据 CSP 的政策和程序以及相关法律法规，确保网络安全要求包含在变更管理方法和程序中以保护信息和技术资产的机密性、完整性和可用性。

编号	具体控制要求	华为云的践行方式
1-5-P-1	应识别、记录和批准 CSP 内变更管理的网络安全要求。	华为云制定了变更管理的管理规定和变更流程，定义了涵盖变更实施前、实施中及实施后应遵循的网络安全要求，以防止未授权变更。例如，变更前，各项变更均需通过多个环节的审核；变更实施中，会通过日志记录、操作监控及双人操作等方式确保变更安全实施，并确保变更过程可追溯；变更后，对变更实施专人验证，确保变更达到预期效果，不会造成网络安全风险。
1-5-P-2	应实施 CSP 内变更管理的网络安全要求。	生产环境的各要素，如网络、系统平台软硬件和应用等的更改，包括架构调整、系统软件更新、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。华为云遵循变更管理的管理规定和变更流程，各项变更均需通过多个环节的审核，需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保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，变更委员会审批通过后才以上线。
1-5-P-3		CSP 变更管理的网络安全应至少包括：
	1-5-P-3-1 在生产系统中安全实施变更（计划工作）的流程和程	华为云制定了规范的变更管理流程，生产环境的各要素发生变更，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

	序，优先考虑网络安全观察。	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。所有变更在申请前，都需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保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。同时华为云制定了更细粒度的变更操作规范，指导整个变更的实施、跟踪以及变更执行后的验证，确保变更达到预期目的。
1-5-P-3-2	网络安全例外变更的实施流程（例如：事件恢复期间的更改）。	华为云也制定了规范的紧急变更管理流程。若紧急变更影响到用户，会按规定的时限提前通过公告、邮件、电话、会议等方式与用户沟通；若紧急变更不满足提前通知的规定，变更将升级至华为云高层领导，并在变更实施后及时对用户公告。此外，华为云针对变更引起现网影响达到事件标准的，要求立刻上报应急小组，进行故障快速恢复。紧急变更均留有记录，在变更执行前保留旧的程序版本及数据，在变更过程中通过双人操作等机制保证变更顺利进行，尽量减少对生产环境的影响。变更实施后，有专人进行验证，确保变更达到预期的目的。
1-5-P-4	定期应用和审查 CSP 内变更管理的网络安全要求。	华为云每年会对建立的变更管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。

6.2 网络安全防御

“网络安全防御”中要求云服务提供商制定网络安全运营和安全管理的策略及流程，包括资产管理、身份与访问管理、信息系统与信息处理设施的保护、密码管理、备份与恢复、网络安全事件管理等方面。相关控制要求及华为云的实践方式如下：

6.2.1 资产管理

确保 CSP 和 CST 拥有准确详细的信息和技术资产清单用以支持组织的网络安全和运营要求并维护信息和技术资产的机密性、完整性和可用性。

编号	具体控制要求	华为云的践行方式
2-1-P-1	除了 ECC 控制 2-1 中的控制之外，CSP 还应至少涵盖以下针对网络安全事件日志与监控管理的网络安全要求的额外控制：	华为云通过 CAM 资产管理系统实时监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理。此外，华为云设置配置经理
	2-1-P-1-1 使用适当技术清点所有信息和技术资产例如配置管理	

	数据库 (CMDB) 或包含所有技术资产清单的类似功能。	对所有业务单元进行配置管理，资源配置模型分为主机、服务树、云基础设施和网络设备，通过构建配置项映射和资源生命周期管理，支撑现网运维获得的稳定和安全，并通过专业的配置管理数据库工具 (CMDB) 对配置项、配置项的属性和配置项之间的关系进行管理。
	2-1-P-1-2 识别资产所有者并让其参与资产管理生命周期。	华为云通过 CAM 资产管理系统实施监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者，明确该资产的所有者将负责该资产的规划、获取、使用、运维到退出等全生命周期的安全职责。华为云通过专业的配置管理数据库工具 (CMDB) 为每个配置项定义责任人，并对配置项、配置项的属性和配置项之间的关系进行管理。

6.2.2 身份与访问管理

确保对信息和技术资产的安全和受限的逻辑访问以防止未经授权的访问，并只允许授权用户完成指定任务所需的访问。

编号	具体控制要求	华为云的践行方式
2-2-P-1	除了 ECC 控制 2-2-3 中的子控制之外，CSP 还应至少涵盖以下针对身份和访问管理要求的网络安全要求的附加子控制：	
	2-2-P-1-1 不能为特定个人分配用于问责的通用帐户凭据身份和访问管理权限。	针对用于审计类的公共专用账号，华为云要求其账号和密码不能分配给特定的个人，账号/权限责任人会审视其负责的专用账号，当不再需要专用账号时修改口令并知会新使用人。
	2-2-P-1-2 安全会话管理，包括会话真实性、会话锁定和会话超时终止。	华为云制定了会话超时策略、账号登陆和锁定策略。其中明确系统支持根据账号、角色、IP 等多种特征组合来确定是否允许通过认证建立认证后的会话，同时必须使用会话 Token 对敏感和关键的操作进行校验以确保会话的真实性。此外管理员在进行系统维护时，查看或检测到非法用户会话时，可通过管理界面强制该用户下线，并清除用户的会话信息。同时设置会话超时机制，在一段时间未收到消息后，可进行会话锁定或返回登录页面，目前超时页面会话为 30 分钟。
	2-2-P-1-3 对特权用户和有权访问云技术堆的人员进行多因素身份验证。	华为云针对特权账号制定了管理要求，将特权账号分类并在特权账号创建、回收、授权、使用、注销等各阶段中遵守管理要求，采用双因子认证对华为云运维人员进行身份认证，如 USB key、Smart Card 等。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。

	2-2-P-1-4 检测和防止未授权访问的正式流程（例如不成功的登录尝试阈值）。	华为云设置了不成功的登录尝试阈值以预防无限制的非法密码登录尝试，目前最大的密码登录尝试次数是5次。对于系统、中间件和网络基础设施的成功和失败的登录尝试均保留日志记录，通过定期的日志审查和日志告警，对非法登录或非法登陆未遂事件进行报告。
	2-2-P-1-5 使用安全方法和算法来保存和处理密码，例如：安全散列函数。	华为云的相关人员遵循华为公司的 IT 安全标准，其中明确不允许以明文形式通过 Internet、无线设备传送密码，密码存储在华为公司系统中时须使用业内认可的加密技术对密码进行加密。此外，华为云要求为用户建立安全的密码重置流程，密码重置应验证用户身份，比如公司邮箱验证码、预留手机号验证码等。
	2-2-P-1-6 第三方人员账户的安全管理。	针对外包合作人员账号/权限，管理负责人为外包合作人员提交申请电子流，并通过相关主管的审批授权，授权完成后内部系统自动为该第三方人员创建一个仅拥有基本权限的内部账号，仅授予完成工作所需要的最低资源访问权限，当第三方人员离场或不再需要账号/权限时该管理负责人也需要提交注销申请。
	2-2-P-1-7 对管理系统、管理控制台实施访问控制。	运维管理平台通过权限管理组赋权，加入权限管理组的申请必须通过对称权限管理组管理员的授权审批。此外，堡垒机通过业务域群组赋权，新增业务域群组的申请必须通过全球运维中心管理员授权审批，在管理员审批通过后堡垒机系统自动创建指定的新业务域群组。员工在申请加入堡垒机业务域群组时必须经过该业务域群组管理员的授权审批，在管理员审批同意后堡垒机系统将该员工加入指定的业务域群组中。
	2-2-P-1-8 屏蔽显示的身份验证输入，尤其是密码，以防止肩窥。	华为云的相关人员遵循华为公司的 IT 安全标准，其中明确采取登录密码输入掩码显示的措施，以防止身份验证密码泄露，造成安全风险。
	2-2-P-1-9 在 CSP 或 CSP 的第三方访问任何 CST 相关资产访问应提前获得 CST 的批准。	华为云不会访问客户的云环境，除非在故障维护时，华为云会在得到运维人员需通过工单系统或书面获得客户授权后，使用指定工具才允许接入租户的控制台或者资源实例以协助客户进行维护，严禁进行超出客户授权范围的任何操作及禁止类的高危操作，或在客户的网络上部署和运行未经客户授权的软件。
	2-2-P-1-10 能够立即中断远程访问会话并阻止某个用户之后的任何访问。	运维平台管理员在进行系统维护时，查看或检测到非法用户会话时，可通过管理界面强制该用户下线，并清除用户的会话信息。同时会通过事后的日志审查，日志告警，对可以用户进行权限清除。
	2-2-P-1-11 为 CSTs 的特权云用户提供多	华为云为客户提供统一身份认证服务（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

	因素身份验证服务。	资源及操作权限。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。用户在密码认证通过后，还将收到一次性短信验证码进行二次认证。用户修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。IAM 结合 PAM 功能还可以更有效地细化管理特权账户。
	2-2-P-1-12 保证对存储系统及方式（如存储区域网络 (SAN)）的限制和受控访问。	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。此外，华为云根据业务功能和网络安全风险将数据中心划分为多个安全区域，实现物理和逻辑控制并用的隔离手段，其中数据存储区部署对象存储系统，提供对象存储服务。在该区域边界由租户在华为云提供的安全组件上配置执行租户所需的访问控制规则，在任意租户空间访问该区域时就不需要绕道 DMZ。但从外网访问，因为安全风险高，所以必须通过 DMZ 的服务控制台或网关才能访问该区。

6.2.3 信息系统和信息处理设施保护

确保信息系统保护和信息处理设施（包括工作站和基础设施）免受网络风险的影响。

编号	具体控制要求	华为云的践行方式
2-3-P-1	除了 ECC 控制 2-3-3 中的子控制之外，CSP 应至少涵盖以下针对信息系统和处理设施保护要求的网络安全要求的附加子控制：	
	2-3-P-1-1 确保根据 CSP 的网络安全标准应用所有配置。	华为云对支撑业务运营的服务器操作系统、数据库管理系统及网络设备建立了统一的基线配置标准，以实现对服务基线配置的统一管理，明确华为云生产环境中各系统/组件的安全配置要求，并确保安全配置的有效执行和持续改进。华为云参考互联网安全中心 (CIS - Center of InternetSecurity) 安全基线并将融入华为云 DevSecOps 流程中并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。华为云的运维团队根据内部的安全基线管理规范，定期检查并更新网络设备安全参数设置。华为云对主机操作系统、虚拟机、数据库、web 应用组件等均进行安全配置加固并进行定期检查。
	2-3-P-1-2 保证数据、	华为云根据业务功能和网络安全风险等级将数据中心

	环境和信息的分离和隔离。	划分为多个安全区域，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威胁的分区自我保护和容错恢复能力。华为云目前将生产及非生产环境划分为多个安全区域，包括：DMZ 区、公共服务区（Public Service）、资源交付区（POD - Point of Delivery）、数据存储区（OBS - Object - Based Storage）、运维管理区（OM - Operations Management）。除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能，确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的 OM 区，攻击面最小，安全风险相对容易控制，并实现内部网络同外部网络的相互隔离及异常流量清洗。
	2-3-P-1-2 跨 CST 系统，以防止数据混合。	华为云从最初的网络架构设计、设备选型配置诸方面进行了综合考虑，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。华为云对云端数据的隔离是通过虚拟私有云（VPC - Virtual Private Cloud）实施的，VPC 采用网络隔离技术，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置：一方面，结合 VPN 或云专线，将 VPC 与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用 VPC 构建私有网络环境，通过子网规划、路由策略配置等进行网络区域划分，将存储放置在内部子网，并通过配置网络 ACL 和安全组规则对进出子网以及和虚拟机的网络流量进行严格的管控。
	2-3-P-1-3 采用遵循最小功能网络安全原则的技术系统配置。	所有产品遵循华为云制定的网络安全红线中基线要求进行网络和系统的配置，确保限制使用不必要的功能，如禁止对 Internet 开发高危服务，不能开放面向 Internet 的高危端口，不能面向 Internet 的接口使用预置口令、空口令或弱口令等。
	2-3-P-1-4 云技术堆栈具有安全处理输入验证、异常和失败的能力。	华为云遵循遵安全及隐私设计原则和规范，在开发阶段就考虑了输入校验错误的需求和设计，确保华为云提供的基础设施具备安全处理输入验证的能力，保障存储、计算等云技术堆栈的安全性。此外，华为云采取完整性校验机制保证系统参数的完整性，如在虚拟机操作系统层面，华为云镜像服务支持镜像完整性检测。在基于镜像创建虚拟机时，系统会自动检查镜像完整性，以确保创建的虚拟机包含完整的镜像内容。
	2-3-P-1-5 将安全功能和应用程序与云技术堆中的其他功能和应用程序完全隔离。	华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，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威胁的分区自我保护和容错恢复能力。华为云目前将生产及非生产环

	<p>境划分为多个安全区域，包括：DMZ 区、公共服务区（Public Service）、资源交付区（POD - Point of Delivery）、数据存储区（OBS - Object - Based Storage）、运维管理区（OM - Operations Management）。为保证租户业务不影响管理操作，确保设备、资源和流量不会脱离有效监管，华为云将其网络的通信平面基于不同业务职能、不同安全风险等级和不同权限需要划分为租户数据平面、业务控制平面、平台运维平面、BMC（Baseboard Management Controller）管理平面、数据存储平面等，以保证关乎不同业务的网络通信流量得到合理且安全的分流，便于实现职责分离。在每个安全区域内，根据所承载业务的隔离要求划分不同网络平面，如 POD 区有租户数据平面、平台运维平面、业务控制平面、BMC 管理平面，而运维区只有平台运维平面和 BMC 管理平面。安全区域与业务平面并用形成更多层面的、既有物理又有逻辑控制的多维度隔离，而这是华为云全栈防护的一部分。</p>
2-3-P-1-6 通知 CST 具有 CSP 提供的可供 CST 使用的网络安全要求。	华为云作为云服务提供商，定义了华为云安全责任共担模型，明确了华为云与客户双方的安全责任边界，和各自应承担的网络安全责任。华为云的各云产品均会为客户提供包括帮助文档、使用手册、安全实施指南等，其中会包含安全指引、安全使用的政策。
2-3-P-1-7 检测和预防对软件和系统的未经授权的更改。	华为云制定了规范的变更管理流程，生产环境的各要素发生变更，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。所有变更在申请前，都需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保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。同时华为云制定了更细粒度的变更操作规范，指导整个变更的实施、跟踪以及变更执行后的验证，确保变更达到预期目的。此外，华为云建立了集中、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，以确保及时对未经授权的活动进行检测和识别。
2-3-P-1-8 完全隔离和保护多个访客环境。	华为云虚拟私有云服务（VPC - Virtual Private Cloud）为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化用户的网络部署。华为云对云端数据的隔离是通过虚拟私有云（VPC - Virtual Private Cloud）实施的，VPC 采用网络隔离技术，实现不同租户间三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置：一方面，结合 VPN 或云专线，将 VPC 与租户内网的传统数据中心互联，实现租户应

	用和数据从租户内网向云上的平滑迁移；另一方面，利用 VPC 的 ACL、安全组功能，按需配置安全与访问规则，满足租户更细颗粒度的网络隔离需要。
2-3-P-1-9 提供给 CST（政府组织和 CNI 组织）的社区云服务应与提供给适用范围之外组织的其他云计算隔离。	<p>作为华为云平台操作系统，华为统一虚拟化平台 (UVP) 通过对服务器物理资源的抽象，将 CPU、内存、I/O 等物理资源转化为一组统一管理、可灵活调度、可动态分配的逻辑资源，并基于这些逻辑资源，在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境。主机内由 Hypervisor 提供的虚拟交换机 (vSwitch) 通过设置 VLAN、VXLAN、ACL 等属性确保虚拟机在网络层的逻辑隔离。同时，UVP 支撑的 CPU、内存、I/O 隔离进一步实现虚拟机在平台层的逻辑隔离。UVP 还提供安全组功能，用于多台虚拟机之间的分组隔离。多台虚拟机之间如果要相互访问，可以建立安全组。同一个安全组内的多台虚拟机默认可相互访问，处于不同安全组的任何两台虚拟机默认禁止相互通信，但可定制配置为允许通信。</p> <p>虚拟私有云服务 (VPC - Virtual Private Cloud) 为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化用户的网络部署。华为云对云端数据的隔离是通过虚拟私有云 (VPC - Virtual Private Cloud) 实施的，VPC 采用网络隔离技术，实现不同租户间三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置：一方面，结合 VPN 或云专线，将 VPC 与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用 VPC 的 ACL、安全组功能，按需配置安全与访问规则，满足租户更细颗粒度的网络隔离需要。</p>
2-3-P-1-10、2-3-P-1-11 从 KSA 内部提供云计算服务，包括用于存储、处理和灾难恢复中心的系统以及用于监控和支持的系统。	华为云会从 KSA 内部提供云计算服务，包括用于存储、处理和灾难恢复中心的系统以及用于监控和支持的系统。此外，华为云提供云监控服务 (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。CES 提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。CES 的监控对象是基础设施的资源使用数据，不监控或触碰租户数据。
2-3-P-1-12 现代技术，例如终端检测和响应 (EDR) 技术，以确保 CSP 的信息处理系统和设备的信息服务器和设备做好对事件进行快速响应的准备。	华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。结合机器学习技术并支持众多威胁分析模型和算法，结合威胁情报和安全咨询，精准识别攻击。并且该系统实时评估华为云安全状态，分析潜在风险，并结合威胁情报进行预警检测未知数据安全风险，做好预防工作并及时采取有效措施进行防御及响应。

6.2.4 网络安全管理

确保对 CSP 和 CST 的保护免受网络风险。

编号	具体控制要求	华为云的践行方式
2-4-P-1	除了 ECC 控制 2-5-3 中的子控制之外, CSP 还应涵盖以下针对网络安全管理的网络安全要求的附加子控制要求, 至少:	
	2-4-P-1-1 监控跨外部和内部网络的流量以检测异常情况。	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。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。
	2-4-P-1-2 云技术堆栈网络与其他内外网的网络隔离和保护。	华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域, 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威胁的分区自我保护和容错恢复能力。华为云目前将生产及非生产环境划分为多个安全区域, 包括: DMZ 区、公共服务区 (Public Service)、资源交付区 (POD - Point of Delivery)、数据存储区 (OBS - Object - Based Storage)、运维管理区 (OM - Operations Management)。除了上述网络分区, 华为云也对不同区域的安全级别进行了划分, 根据不同的业务功能, 确定不同的攻击面以及不同的安全风险, 比如说直接暴露在互联网的区域, 安全风险最高, 而与互联网几乎没有交互并且不向其他区域开放接口的 OM 区, 攻击面最小, 安全风险相对容易控制, 并实现内部网络同外部网络的相互隔离及异常流量清洗。
	2-4-P-1-3 防止拒绝服务攻击 (包括分布式拒绝服务 (DDoS))。	华为云在网络边界部署 DoS/DDoS 防范清洗层、下一代防火墙、入侵防御系统层以及网站应用防火墙层。通过限制虚拟端口的连接跟踪数来抵御来自云平台外部或平台内部其他虚拟机的大流量攻击, 此类攻击会产生大量连接跟踪表项, 如果不做限制, 会耗尽连接跟踪表资源, 导致不能接受新的连接请求, 最终导致业务及管理流量中断。除此之外, 还为客户提供了解析 Anti-DDoS 流量清洗服务, 客户可将 Anti-DDoS 流量清洗设备部署在其数据中心网络出口区域。Anti-DDoS 设备通过对互联网访问弹性云服务器、弹性负载均衡和裸金属服务器的业务流量进行实时监测, 及时发现异常 DDoS 攻击流量。在不影响正常业务的前提下, 可以通过调整连接跟踪数, 有效缓解大流量攻击对业务的影响。

	<p>提下，根据用户配置的防护策略，清洗掉攻击流量。</p>
2-4-P-1-4 保护通过网络传输的数据； 使用加密原语进出云技术堆栈网络； 用于管理和行政访问。	<p>华为云建立了保护技术设备上的数据的加密策略与密钥管理机制，对加密级别、加密方法进行了规定。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，传输中数据的保护通过如下方式提供：</p> <ol style="list-style-type: none"> 1. 虚拟专用网络（VPN）：用于在远端网络和 VPC 之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云。目前，华为云采用硬件实现的 IKE（密钥交换协议）和 IPSecVPN 结合的方法对数据传输通道进行加密。 2. 应用层 TLS 与证书管理：华为云服务提供 REST 和 Highway 方式进行数据传输。 以上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。 此外，华为云运维人员心对接客户 VPC 环境时，采用安全传输协议 HTTPS，以防止数据在传输过程中发生泄露。
2-4-P-1-5 不同网段之间的访问控制。	<p>华为云根据业务功能和网络安全风险将数据中心划分为多个安全区域，实现物理和逻辑控制并用的隔离手段，包括：DMZ 区、公共服务区（Public Service）、资源交付区（POD - Point of Delivery）、数据存储区（OBS - Object - Based Storage）、运维管理区（OM - Operations Management）。除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能，确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的 OM 区，攻击面最小，安全风险相对容易控制，并实现内部网络同外部网络的相互隔离及异常流量清洗。此外，虚拟私有云（VPC - Virtual Private Cloud）为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，提升客户云中资源的安全性，简化用户的网络部署。客户可以根据其在华为云上的网络安全需求在网络 ACL 和安全组中定义访问控制规则：</p> <ul style="list-style-type: none"> ● 网络 ACL：网络 ACL 是对一个或多个子网的访问制定、维护并执行访问控制策略的系统，根据与子网关联的入站/出站规则，判断数据包是否被允许流入/流出关联子网。 ● 安全组：在 VPC 中，安全组是一组对弹性云服务器的访问规则的集合，为同一个 VPC 内具有相同安全保护需求并且相互信任的弹性云服务器提供访问策略。用户可以自行创建并定义安全组内与组间弹性

		云服务器的访问规则，将 VPC 中的弹性云服务器划分成不同的安全域，以提升弹性云服务器访问的安全性。
	2-4-P-1-6 云服务交付网络、云管理网络和 CSP 企业网络之间的隔离。	<p>华为云根据业务功能和网络安全风险将其平台划分为多个安全区域，实现物理和逻辑控制并用的隔离手段，提供网络面对外部入侵时的自我保护和容错恢复能力。以下为华为云五个重要的安全区域：</p> <ul style="list-style-type: none"> ● DMZ 区：为客户部署了面向外网和用户的前置部件，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。用户对 DMZ 区的访问行为不可信，所以华为云 HCSO 为客户单独隔离 DMZ 区域。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）及入侵检测设备（IPS）以保护基础網路、平台及应用。 ● 公共服务区：该区域主要部署 IaaS/PaaS/SaaS 服务化组件如 IaaS/PaaS/SaaS 服务控制部件，以及一些基础设施服务部件如补丁服务等。此区域内的部件根据业务需要由华为云受限开放给用户。客户云管理员可以从内网区访问该区域进行操作和管理。 ● 资源交付区（POD）：在此区域部署提供客户所需的基础设施资源，包括计算、存储、网络资源，如虚拟机、磁盘、虚拟网络。该区域还可以支撑对进出互联网的客户流量做 DDoS 防护及入侵检测与防御，保障客户业务安全。 ● 数据存储区：此区域部署对象存储系统，提供对象存储服务。由于存储客户隐私数据，所以进行了分区隔离。在该区域边界由客户在安全组件上配置执行所需的访问控制规则，在任意客户空间访问该区域时不需要绕道 DMZ。但由于从外网访问安全风险高，所以必须通过 DMZ 的服务控制台或网关才能访问该区。 ● 运维管理区：该区域主要部署操作运维部件，管理员可以通过此区域对其他区域进行统一的业务系统运维运营管理。当客户选择使用华为云提供的统一运维运营服务时，华为云运维人员将通过 VPN 接入该区域，再通过堡垒机访问被管理节点。

6.2.5 移动设备安全

确保保护移动设备（包括笔记本电脑、智能手机和平板电脑）免受网络风险，并确保在使用移动设备时安全处理 CSP 和 CST 的信息（包括敏感信息）。

编号	具体控制要求	华为云的践行方式

2-5-P-1	除了 ECC 控制 2-6-3 中的子控制之外, CSP 还应至少涵盖以下针对移动设备安全的网络安全要求的附加子控制:		
	2-5-P-1-1 所有终端用户和移动设备的清单。	华为云使用 MDM 移动设备管理系统以实施对移动计算设备的统一管理, 记录和维护所有终端用户和移动设备的清单, 对移动设备进行分类、监控和管理。	
	2-5-P-1-2 集中式移动设备安全管理。	华为云使用 MDM 移动设备管理系统以实施对移动计算设备的统一管理, 记录和维护所有终端用户和移动设备的清单, 对移动设备进行分类、监控和管理。	
	2-5-P-1-3 终端用户设备的屏幕锁定。	华为云制定并实施办公场所安全管理规定, 对员工的安全责任与行为规范提出要求, 要求终端用户设备须设置自动锁屏功能, 锁屏生效时间不应大于 10 分钟。	
	2-5-P-1-4 终端用户设备的数据清理和安全处置, 尤其是接触过云技术堆栈的人。	员工离职或转岗时, 必须对办公计算机硬盘进行格式化处理, 若涉及机密、绝密信息, 应确保删除的数据无法恢复, 同时主动及时的卸载 BYOD 上公司应用清除公司数据。若设备丢失或被盗, 员工须向业务主管和信息安全部门报告, 并远程擦除公司数据, 并取消设备绑定。	

6.2.6 数据和信息保护

根据组织政策和程序以及相关法律法规, 确保 CSP 和 CST 数据和信息的机密性、完整性和可用性。

编号	具体控制要求	华为云的践行方式
2-6-P-1	除了 ECC 控制 2-7-3 中的子控制之外, CSP 还应至少涵盖以下针对数据和信息保护的网络安全要求的附加子控制要求:	
	2-6-P-1-1 禁止生产环境之外的任何环境中使用云技术堆栈的数据, 除非在应用之后严格控制保护该数据, 例如: 数据脱敏或数据扰频技术。	华为云研发环境采取分级管理, 对开发环境进行包括物理隔离、逻辑隔离、接入访问控制、数据传输通道审批及审计等保护措施。并且严格控制未脱敏的数据流入测试环境, 避免生产数据或未脱敏的生产数据用于测试, 使用完成后需要进行数据清理。
	2-6-P-1-2 向 CST 提供安全数据存储流程、程序和技术, 以符合相关法律和监管的要求。	华为云遵从 CST 所在国家或地区的安全法规以及行业监管要求的基础上, 参考业界最佳实践从组织、流程、规范、技术、合规、生态和等方面建立并管理完善、高可信、可持续的数据安全保障体系。华为云为保护租户数据的存储安全采取了一系列的保护机制。客户可选用 DEW 服务对存储的数据进行加密。DEW 负责对密钥全生命周期进行集中管理。在未授权的情

		况下，除客户外的任何人都无法获取密钥，对数据进行解密。此外，华为云提供了密钥管理服务（KMS），它帮助用户集中管理密钥，保护密钥安全。它通过使用硬件安全模块（HSM - Hardware Security Module），为租户创建和管理密钥，防止密钥明文暴露在 HSM 之外，从而防止密钥泄露。目前，华为云云硬盘（EVS）、对象存储服务（OBS）、镜像服务（IMS）和关系型数据库等多个服务均提供数据加密（服务端加密）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。
2-6-P-1-3 在与 CSP 的合同终止或到期时，应以安全的方式处理 CST 的数据。		在客户确认删除数据后，华为云会对指定的数据及其所有副本进行全面的清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。
2-6-P-1-4 承诺根据相关法律法规要求维护 CST 数据和信息的机密性。		华为云恪守“不碰数据”底线，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令，此外华为云运维人员需通过工单系统或书面获得客户授权后，使用指定工具才允许接入租户的控制台或者资源实例以协助客户进行维护，严禁进行超出客户授权范围的任何操作及禁止类的高危操作，或在客户的网络上部署和运行未经客户授权的软件，以确保 CST 数据和信息的机密性。华为云严格遵守《CCC》所述的网络安全原则。
2-6-P-1-5 为 CST 提供安全的方式来导出和传输数据和虚拟基础设施。		在服务协议终止时，客户可通过华为云提供的云数据迁移服务（CDM），将内容数据从华为云中迁移出去，如迁移至本地数据中心。在传输过程中使用高版本 TLS 加密协议保障数据安全，确保不同状态下的数据的机密性。使用数字签名和时间戳等控制机制，防止数据传输过程中被篡改，确保信息完整性并防止重放攻击。

6.2.7 密码学

根据政策、程序和相关法律法规，确保正确有效地使用密码学来保护信息资产。

编号	具体控制要求	华为云的践行方式
2-7-P-1	除了 ECC 控制 2-8-3 中的子控制之外，CSP 还应至少涵盖以下附加的加密子控制：	

	2-7-P-1-1 符合国家密码标准（NCS-1:2020）先进水平的强加密技术机制和密码学原语。	华为云制定并实施密码算法应用规范，规范了密码算法的选择规则及应用规则，并给出常见应用实例指导。华为云使用的密码算法均包含在沙特国家密码标准中。目前，华为云硬盘（EVS）、对象存储服务（OBS）、镜像服务（IMS）和关系型数据库等多个服务均采用高强度的算法对存储的数据进行加密，满足沙特国家密码标准要求。
	2-7-P-1-2 使用安全认证机构的方式或来自受信任认证机构的证书。	华为云制定了证书管理规范，明确云平台统一采用华为云 PKI 系统颁发的数字证书，对外的业务采用受信的商业数据证书。所有数字证书均纳入华为云证书管理系统进行统一管理，严禁产品或个人独自建立华为云根 CA 系统或子 CA 系统，并使用这些自建的 CA 对外发布数字证书。

6.2.8 备份与恢复管理

根据组织政策和程序以及相关法律法规，确保保护 CSP 的数据和信息，包括信息系统和软件配置，免受网络风险。

编号	具体控制要求	华为云的践行方式
2-8-P-1	除了 ECC 控制 2-9-3 中的子控制之外，CSP 还应至少涵盖以下针对备份和恢复管理的网络安全要求的附加子控制：	
	2-8-P-1-1 保护 CST 数据备份及其介质的访问、存储和传输，并保护其免受损坏、修改或未经授权的访问。	华为云提供的基础设施存储、数据库本身具有数据备份的机制，备份的数据副本和数据采用同样的数据安全措施。例如云硬盘提供安全的加密算法（AES-256）和功能、对象存储服务可提供服务端加密功能及防盗链功能、RDS 数据库提供存储加密机制等。通过与数据加密服务集成，备份数据可以方便、快速地实现加密存储，有效保证备份数据的安全性。客户使用 VBS 云硬盘备份服务、云服务器备份服务等进行备份，加密盘的加密数据自动加密，保证数据安全。
	2-8-P-1-2 保护云技术堆栈备份的访问、存储和传输及其媒介，并保护其免受损坏、修改或未经授权的访问。	华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。华为云，建立了节点数据备份机制，通过 eBackup 系统实现对节点数据的备份，且备份失败时自动通过邮件发送给备份管理员进行跟进。

6.2.9 漏洞管理

确保及时发现和有效补救技术漏洞，以防止或尽量减少利用这些漏洞对 CSP 和 CST 发起网络攻击的可能性。

编号	具体控制要求	华为云的践行方式
2-9-P-1	除了 ECC 控制 2-10-3 中的子控制之外，CSP 还应至少涵盖以下针对漏洞管理要求的网络安全要求附加子控制：	
	2-9-P-1-1 至少每月评估和修复云技术堆栈外部组件的漏洞并至少每三个月修复一次云技术堆栈内部组件的漏洞。	华为云建立了漏洞定期扫描机制，每月对报告范围内的产品执行漏洞扫描并由漏洞扫描团队负责对扫描结果进行跟踪处理。同时，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。华为云已建立起从漏洞感知到现网修复的端到端漏洞响应工单系统，自动根据漏洞的严重程度确定处理优先级，从而明确对应的漏洞修复 SLA 要求，以尽快修复为原则。对于重大安全漏洞，安全运维团队可通过自研工具，对现网进行扫描，实现分钟级的受影响服务和模块的范围界定。
	2-9-P-1-2 向 CST 通报可能影响他们的已识别漏洞，以及已经采取的保护措施。	华为云安全运维团队会根据现网情况，采取必要的漏洞缓解措施，例如限制端口访问、实施 WAF 漏洞规则等方式对受影响的服务进行防护或隔离，以降低漏洞被利用的风险。对于需要通过版本、补丁修复的漏洞，通过灰度发布或蓝绿部署等方式尽量减少对租户业务造成影响。同时，华为云还持续更新操作系统及容器镜像，通过镜像和容器的滚动升级完成系统漏洞修复，不会对租户业务造成影响。此外，华为云针对会影响客户服务的漏洞，华为云会发布漏洞公告，其中包括漏洞详情、漏洞原理分析、漏洞影响范围、漏洞防范措施及漏洞解决方法等内容。

6.2.10 渗透测试

通过模拟网络攻击方式评估 CSP 网络安全防御能力的效率，以发现技术基础设施中可能导致网络漏洞的未知弱点。

编号	具体控制要求	华为云的践行方式
2-10-P-1	除了 ECC 控制 2-11-3 中的子控制之外，CSP 还应至少涵盖以下针对渗透测试的网络安全要求的附加子控制：	
	2-10-P-1-1 渗透测试的范围必须涵盖云技术堆栈，且必须至少每六个月进行一次。	华为云建立了渗透测试与漏洞扫描管理规定，明确了华为云平台开展渗透测试时应遵循的安全要求，规范渗透测试行为，确保渗透测试活动合规与受控。华为云每半年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，渗透测试报告及跟进情况会通过内部审计以及外部认证机构核查。
--	--	---

6.2.11 网络安全事件日志与监控管理

确保及时收集、分析和监控网络安全事件日志，主动检测和有效管理网络攻击，以防止或尽量减少对 CSP 和 CST 业务的影响。

编号	具体控制要求	华为云的践行方式
2-11-P-1	除了 ECC 控制 2-12-3 中的子控制之外，CSP 还应至少涵盖以下针对网络安全事件日志和网络安全要求的附加子控制管理：	
	2-11-P-1-1 开启和保护云技术堆栈的事件日志和审计跟踪。	华为云建立了集中、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，持续的监控和实时分析保证对安全事件的及时发现，以确保支撑网络安全事件回溯。
	2-11-P-1-2 开启和收集尝试登录的历史记录。	运维平台作为华为云进行运维管理的入口，开启了录屏及高危命令限制功能，通过系统控制降低异常操作的几率。此外，堡垒机还开启了操作日志记录功能，操作日志无法被人为修改，日志记录包括登录 IP、登录方式及登录时间等。
	2-11-P-1-3 开启和保护 CSP 在租户级别执行的活动和操作的所有事件日志，以支持取证分析。	华为云不会访问客户的云环境，除非在故障维护时，华为云会在得到运维人员需通过工单系统或书面获得客户授权后，使用指定工具才允许接入租户的控制台或者资源实例以协助客户进行维护，严禁进行超出客户授权范围的任何操作及禁止类的高危操作，或在客户的网络上部署和运行未经客户授权的软件。内部人员运维操作均被日志平台采集并记录，华为云有专门的内审部门，定期对运维流程各项活动进行审计。
	2-11-P-1-4 根据法规或法律要求，保护网络安全事件日志免遭更改、披露、破坏及未经授权的访问和未经授权的发布。	在日志保存过程中采取安全措施防止日志被篡改，以确保支撑网络安全事件回溯和合规。为确保日志数据安全，安全日志会进行统一备份或归档，并依照数据安全管理的要求，限制安全日志使用的申请及权限，仅允许授权人员因必要原因进行安全日志的查询，确保受控使用。华为云遵从法律法规要求，具备集中、完整的日志审计系统，具备强大的数据保存及查询能力，确保所有日志内容保存时间超过 6 个月。
	2-11-P-1-5 使用涵盖完整云技术堆栈的	华为云建立了集中、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

	SIEM 技术进行持续网络安全事件监控。	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，以确保支撑网络安全事件回溯。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM - Security Information and Event Management）系统如 ArcSight、Splunk 对接。
2-11-P-1-6	定期审查涵盖云技术堆栈中的 CSP 事件的网络安全事件日志和审计跟踪。	对于集中存储安全日志的日志分析平台，系统管理员会定期例行对采集状态、存储状态进行检查，保证安全日志的可用性。华为云日志分析平台对产品相关运维系统、服务器及网络设备的安全日志进行了收录，同时在平台内预设了异常操作规则，用于识别用户进行异常操作的情形，自动生成告警信息并推送至相关安全部门进行后续跟进处理，异常告警按照服务等级协议要求及时处理并通过事件分析处理平台进行实时大屏监控与记录。
2-11-P-1-7	远程访问会话事件日志的自动监控和记录。	华为云的统一日志分析平台，对 SVN、堡垒机、主机、WAF、HSS 等服务的安全日志进行收集并建立日志监控自动告警机制。运维平台作为华为云进行运维管理的入口，开启了操作日志记录的功能，操作日志无法被人为修改，且至少保留了 6 个月的日志记录，包括登录 IP、登录方式及登陆时间等。
2-11-P-1-8	安全处理审计跟踪和网络安全事件日志中发现的用户相关数据。	华为云建立了安全日志管理规范，其中明确安全日志中不应记录敏感的个人数据，如日志中包含个人数据且与网络安全威胁直接相关且必要的信息，应遵循最小化原则，并且保证对日志的安全措施不低于日志所包含的个人数据的保护措施，须进行数据加密或匿名化处理，防止应用或个人通过日志获取用户的个人信息。

6.2.12 网络安全事件与威胁管理

确保及时识别和检测网络安全事件及其对网络安全威胁的有效管理和主动响应，以防止或最大限度地减少对 CSP 业务造成的影响。

编号	具体控制要求	华为云的践行方式
2-12-P-1	除了 ECC 控制 2-13-3 中的子控制之外，CSP 还应至少涵盖以下针对网络安全事件和威胁管理的网络安全要求的附加子控制： 2-12-P-1-1 订阅已授权的专业组织和团体以及时了解网络安全威胁、通用实践和关键知识。	华为云 PSIRT 会主动监控业界知名漏洞库、安全论坛、邮件列表、安全会议等渠道，以保证第一时间感知到包括云在内的华为相关漏洞信息。华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。支持众多威胁分析模型和算法，

		结合威胁情报和安全咨询，精准识别攻击，并且该系统实时评估华为云安全状态，分析潜在风险，并结合威胁情报进行预警，做好预防工作。
2-12-P-1-2 培训员工和第三方人员应对与其角色和职责相符的网络安全事件。		华为云通过公司统一开展的年度例行学习、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，其中包含信息安全事件报告责任。此外，华为云每年对信息安全事件管理程序和流程进行培训和测试，所有的安全事件响应人员，包括后备人员均需参与。
2-12-P-1-3 定期测试事件响应能力。		华为云每年对信息安全事件管理程序和流程进行培训和测试，所有的安全事件响应人员，包括后备人员均需参与。此外，华为云针对各产品可能涉及的不同突发场景，规范了应急响应工作流程，形成应急响应预案，定期做应急演练和测试，持续优化应急响应机制。
2-12-P-1-4 网络安全事件的根本原因分析并制定解决方案。		华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划和流程，作为流程的一环节，在安全事件得到遏制后，华为云会做根本原因分析，并制定应对和预防措施。同时，华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。此外，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。
2-12-P-1-5 根据相关法律和监管要求，在案件的法律诉讼和取证中支持 CST，保护属于 CSP 管理和责任的监管链。		华为云制定了安全事件应急处置流程及响应流程，当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。此外，华为云会遵从与客户订的协议中约定的要求，会安排专人积极配合客户的需求。
2-12-P-1-6 向 CST 实时报告已被发现的可能影响 CST 的事件。		华为云针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。华为云设置 7*24 的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。
2-12-P-1-7 支持 CST 根据 CSP 和 CST 之间的协议处理安全		针对影响客户的安全事件，华为云建立了完善的事件通告机制。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的

	事件。	时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。
	2-12-P-1-8 衡量与监控网络安全事件指标并检查其对合同和立法要求的合规情况。	华为云会定期对事件的相关指标进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。此外，华为云每年对高风险事件处理过程中的各项指标进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求以及合同或监管立法的要求。

6.2.13 物理安全

确保 CSP 的信息和技术资产免受未经授权的物理访问、丢失、盗窃和损坏。

编号	具体控制要求	华为云的践行方式
2-13-P-1	除了 ECC 控制 2-14-3 中的子控制之外，CSP 还应至少涵盖以下针对物理安全的网络安全要求的附加子控制：	
	2-13-P-1-1 持续监控对 CSP 站点和建筑物的访问。	华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。
	2-13-P-1-2 防止未经授权访问云技术堆栈中的设备。	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。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。
	2-13-P-1-3 通过采用相关立法和最佳实践处置云基础设施硬件，尤其是存储设备（外部或内部）。	华为云使用包含存储介质的设备由专人管理，使用完毕后由专人对其进行格式化处理。存储公司保密信息的存储介质报废时由专人确保其上存储的信息均被清除且不可恢复，处理方式包括消磁、物理销毁或低级格式化。当物理磁盘报废时，华为云通过对存储介质进行消磁、折弯或破碎等方式清除数据，并对数据清除操作保存完整记录，满足行业标准，确保用户隐私和数据不受未授权访问。

6.2.14 Web 应用安全

确保 CSP 的外部 Web 应用程序免受网络风险。

编号	具体控制要求	华为云的践行方式
2-14-P-1	<p>除了 ECC 控制 2-15-3 中的子控制之外, CSP 还应至少涵盖以下针对 Web 应用程序安全的网络安全要求附加子控制:</p> <p>2-14-P-1-1 保护应用服务交互中涉及的信息免受可能的风险(例如: 不完整的传输、错误的路由、未经授权的消息更改、未经授权的披露...)。</p>	<p>华为云对在公共网络上提供的应用服务采用多重机制和措施进行重点保护。</p> <ul style="list-style-type: none"> 身份认证及鉴权: 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。华为云 API 网关对用户命令支持二级权限管理。用户发出命令时, 不仅需要通过 IAM 的身份登录和鉴权, 而且命令也需要经过 API 网关的检查鉴权。平台层或应用层接到命令后, 会再次对用户的权限进行检查判断, 只有用户确实拥有当前 API 命令的执行权限, 命令才允许执行。所有的访问请求可以通过令牌和访问密钥两种方式认证。 传输保护: API 调用需使用 TLS 加密以保证传输的机密性。目前 API 网关所有对外网开放的 API 均使用 TLS 1.2 版本加密协议, 并且支持 PFS (Perfect Forward Secrecy) 安全特性。 边界防护: API 网关结合 Anti-DDoS、IPS 和 WAF 等多层高级边界防护机制针对不同的威胁和攻击进行有效防范。通过负载均衡器对 TLS 加密传输进行解密, 多层高级边界防护机制可对 API 网关流量明文进行监控, 对攻击执行阻断。 API 流量控制: API 网关实现对用户调用 API 的频率的适当流量控制, 确保基于 API 的访问的高可用性和连续性。API 网关提供针对 API 级别和云服务客户级别的秒级流控配置。每个开放的 API 在 API 网关需要配置对应的流控信息, 在单位时间内, 每个 API 基于所有云服务客户调用该 API 次数的配额、每个云服务客户调用该 API 次数的配额分别进行流控。

6.2.15 密钥管理

确保对 CSP 和 CST 的加密密钥进行安全管理, 以保护信息和技术资产的机密性、完整性和可用性。

编号	具体控制要求	华为云的践行方式
----	--------	----------

2-15-P-1	应识别、记录和批准 CSP 内密钥管理过程的网络安全要求。	华为云制定并实施密钥管理安全规范，对密钥生命周期各阶段的安全进行管理，明确在密钥生成、传输、使用、存储、更新、备份与恢复、销毁等阶段的安全管理要求。
2-15-P-2	应实施 CSP 内密钥管理过程的网络安全要求。	华为云各业务领域须遵照密钥管理安全规范，对密钥生成、密钥存储、密钥分发、密钥更新和密钥销毁等操作实施安全管控，防止密钥泄露和密钥丢失损坏。同时，华为云使用密钥管理服务（KMS）管理 RDS 和 OBS 用户的主密钥，RDS 和 OBS 通过调用 KMS 的内部接口请求使用主密钥用于加解密工作。
2-15-P-3	除了 ECC 子控制 2-8-3-2 之外，CSP 内密钥管理的网络安全要求应至少包括以下内容：	<p>2-15-P-3-1 确保明确定义加密密钥的所有权。</p> <p>2-15-P-3-2 实施安全的密钥检索机制，以防密钥丢失（例如密钥备份和可信密钥存储的实施，严格在云外部）。</p> <p>2-15-P-3-3 开启和监控密钥的所有审计跟踪。</p>
2-15-P-4	应定期审查 CSP 内密钥管理的网络安全要求。	华为云每年会对建立的密钥安全相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。

6.2.16 系统开发安全

确保以安全的方式开发、集成和部署 CSP 系统。

编	具体控制要求	华为云的践行方式

号		
2-16-P-1	应识别、记录和批准 CSP 内系统开发的网络安全要求。	华为云已制定开发安全管理相关制度，对华为云服务在规划、设计、开发、部署、运维和用户支撑环境应遵循的安全编程规范及应用安全开发规范进行了定义。
2-16-P-2	应实施 CSP 内系统开发的网络安全要求。	华为云及相关云服务遵从安全及隐私设计原则和规范、法律法规要求，在安全需求分析和设计阶段根据业务场景、数据流图、组网模型进行威胁分析。当识别出威胁后，设计工程师会根据削减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求、安全功能，并根据公司的测试用例库完成安全测试用例的设计，确保落地，最终保障产品、服务的安全。
2-16-P-3	CSP 内系统开发的网络安全要求应至少包括开发生命周期中的以下控制：	<p>2-16-P-3-1 在设计和实施云计算服务时考虑云技术栈和相关系统的网络安全要求。</p> <p>华为云通过完善的制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全需求分析、安全设计、安全编码和测试、安全验收和发布、漏洞管理等环节。</p> <ul style="list-style-type: none"> 针对各产品，新的研发需求须经过需求分析团队的审批后才能进入开发环节。此外，针对涉及新服务构建的重要研发需求，会执行立项评审。新的产品或服务转公测或正式商用前，华为云会对产品的生产环境进行生产就绪程度评审，以满足业务要求。 华为云及相关云服务遵从安全及隐私设计原则和规范、法律法规要求，在安全需求分析和设计阶段根据业务场景、数据流图、组网模型进行威胁分析。当识别出威胁后，设计工程师会根据削减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求、安全功能，并根据公司的测试用例库完成安全测试用例的设计。 华为云引入了静态代码扫描工具每日检查，其结果数据进入云服务持续集成和持续部署工具链，通过质量门限进行控制，以评估云服务产品的质量。 所有云服务发布前都经过了多轮安全测试，测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。 华为云建立了一系列静态代码扫描工具，确保涉及开发的产品变更在上线前经过代码审核验收。华为云建立了正式的内部测试及验收措施，以确保仅适当且经过授权的变更被发布至生产环境。 <p>2-16-P-3-2 保护系统</p> <p>华为云规范了研发环境的信息安全通用管理要求，以</p>

	开发环境、测试环境（包括测试环境中使用的数据）和集成平台。	及环境规划、建设、使用、维护、撤销中的信息安全管理。同时华为云规范了采用 DevOps 开发模式的产品/服务在部署和发布阶段流程，当中规范了对环境隔离的相关要求，通过验证测试后的软件产品需按照业务需求及技术要求、发布策略限制分批部署到生产环境，以确保对生产环境的变更得到有效控制，提高生产环境稳定性。生产数据用于测试环境之前，需去除生产数据中的认证凭证数据（如密码、密钥）和保密的业务数据（如定价信息），并对生产数据中的个人数据进行匿名化处理。禁止未经授权打通测试环境和生产环境的网络链接，避免因测试环境被入侵而导致生产环境安全风险。
2-16-P-4	应定期应用和审查 CSP 内系统开发的网络安全要求。	华为云每年会对建立的安全开发、安全测试等安全开发生命周期相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。

6.2.17 存储介质安全

确保 CSP 安全处理物理介质上的信息和数据。

编号	具体控制要求	华为云的践行方式
2-17-P-1	应识别、记录和批准在 CSP 内信息使用和数据介质的网络安全要求。	华为云制定并实施移动介质管理规定，各类移动介质由专人管理，借用时需要审批，使用完毕后须进行格式化处理。对个人存储介质及数字设备进出不同安全保密级别的区域及其使用均制定了不同的安全要求。
2-17-P-2	应实施 CSP 内信息使用和数据介质的网络安全要求。	华为云遵循已建立的移动介质管理要求，对存储组织信息的介质按照其对组织的重要程度实施适当水平的保护，以及防止存储在介质中的信息遭受未授权的泄露、修改、移除或破坏。
2-17-P-3	在 CSP 内信息使用和数据介质的网络安全要求应至少包括以下内容：	
	2-17-P-3-1 在处置或再利用之前强制执行介质消毒。	华为云制定并实施介质管理规定，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，并对销毁操作进行记录。存储公司保密信息的存储介质报废时由专人确保其上存储的信息均被清除且不可恢复，处理方式包括消磁、物理销毁或低级格式化。
	2-17-P-3-2 清除介质时使用安全方法。	对于物理存储介质销毁的情况，须在华为员工的全程监督的情景下实施，通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，使其上的数据无法恢复。

	2-17-P-3-3 用于维护可移动介质上数据的机密性和完整性的规定。	华为云制定并实施介质管理规定，对于存储公司保密信息的存储介质或保管备份的存储介质应对其进行加密，同时通过存放在受控访问区域对存储介质的出入进行访问控制限制和防止出现非法访问和使用，保障移动介质上的数据机密性和完整性。
	2-17-P-3-4 可读的介质标签，解释其分类及其所含信息的敏感性。	华为云要求包含华为公司保密信息的存储介质必须进行标记。保密数据应依据数据密级进行标记或者贴上标签，须说明其保密级别。对于运输过程中的介质或授权存放介质的设施外部必须贴标签，对用于运输介质的上锁容器，其外部也必须贴有标签。
	2-17-P-3-5 可移动介质的受控和物理安全存储。	华为云要求存储介质必须保存在受控访问区，或者放置在公司内部上锁的柜子里，存储介质从受控区域出入的时候必须对出库到入库的具体信息对账和闭环跟踪。各类移动介质由专人管理，借用时需要审批，使用完毕后须进行格式化处理。对个人存储介质及数字设备不允许带入有特殊保密要求的区域。
	2-17-P-3-6 限制和控制云技术堆栈内便携式介质的使用。	华为云制定了存储介质及设备进出机房管理规定，要求存储介质及设备进出机房前需进行登记并得到授权。物理存储介质进出机房时均会进行数据防泄漏管理，并对数据擦除、报废清退流程进行规定，减少可能存在的数据泄露损失。此外，华为云规定不得用个人存储介质连接服务器，未经授权，也不得私自使用任何存储介质连接服务器。
2-17-P-4	应定期应用和审查在CSP内信息使用和数据介质的网络安全要求。	华为云每年会对建立的移动介质管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全管理的策略、标准、规范和具体措施在各业务领域的流程落地。

6.3 网络安全弹性

“网络安全弹性”为云服务提供商实施有效的业务连续性管理提供了实施指引，涵盖业务连续性计划的开发、应急响应计划及灾难恢复计划的实施等方面。相关控制要求及华为云的实践方式如下：

6.3.1 业务连续性管理 (BCM) 的网络安全弹性

确保将网络安全弹性要求纳入 CSP 和 CST 的业务连续性管理中，并补救和尽量减少因网络安全事件对系统、信息处理设施和关键电子服务的影响。

编号	具体控制要求	华为云的践行方式

3-1-P-1	除了 ECC 控制 3-1-3 中的子控制之外, CSP 还应至少涵盖以下针对业务连续性管理的网络安全弹性方面的网络安全要求附加子控制:	
	3-1-P-1-1 以安全的方式制定和实施灾难恢复和业务连续性程序。	华为云制定了业务连续性管理规定, 以规范业务连续性相关管理框架、目的和范围、管理目标、角色和职责等内容。华为云已经通过 ISO22301 业务连续性管理体系标准的认证, 并制定了业务连续性计划, 其中包含了自然灾害、事故灾害、信息技术风险等突发事件的应对策略与应对流程。此外, 华为云还制定了灾难恢复计划, 并定期对其进行测试。例如, 将一个地理位置或区域的云平台基础架构和云服务处于离线状态, 模拟一个灾难, 然后按照灾难恢复计划进行系统处理和转移, 以验证故障位置的业务及营运功能, 测试结果将被注释并记录归档, 用以持续改进该计划。
	3-1-P-1-2 制定和实施程序以确保专用于保护云技术堆栈的网络安全系统的弹性和连续性。	华为云针对各云服务和云产品, 如 WAF、DDoS 等, 可能涉及的不同突发场景, 规范了应急响应工作流程, 形成应急响应预案。同时, 华为云每年会在组织内进行业务连续性的宣传和培训, 以及定期做应急演练和测试, 持续优化应急响应机制。此外, 华为云还制定了灾难恢复计划, 并定期对其进行测试。例如, 将一个地理位置或区域的云平台基础架构和云服务处于离线状态, 模拟一个灾难, 然后按照灾难恢复计划进行系统处理和转移, 以验证故障位置的业务及营运功能, 测试结果将被注释并记录归档, 用以持续改进该计划。

6.4 第三方网络安全

“第三方网络安全”为云服务提供商实施供应商或第三方管理提供了指引。控制要求覆盖服务供应商的网络安全能力、第三方安全等领域。相关控制要求及华为云的实践方式如下:

6.4.1 供应链与第三方网络安全

根据政策和程序以及相关法律法规, 确保资产免受与第三方相关的网络安全风险, 包括外包和托管服务。

编号	具体控制要求	华为云的践行方式
4-1-P-1	除了实施 ECC 控制措施 4-1-2 和 4-1-3 之外, CSP 还应至少涵盖以下第三方网络安全要求的附加子控制措施:	
	4-1-P-1-1 确保 CSP 满足 NCA 的要求, 删除由 CST 市场的	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。华为云对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案, 在

	第三方供应商提供的可能对国家组织构成网络安全威胁的软件或服务。	选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件退出等环节，均实施严格的管控。例如在选型分析环节，增加开源软件选型阶段的网络安全评估要求，严管选型。在使用中，须将第三方软件作为服务或解决方案的一部分开展相应活动，并重点评估开源及第三方软件和自研软件的结合点，或解决方案中使用独立的第三方软件是否引入新的安全问题。
4-1-P-1-2 要求供应商和第三方供应商的任何设备或服务提供安全文档。	4-1-P-1-2 要求供应商和第三方供应商的任何设备或服务提供安全文档。	华为云作为云服务提供商，定义了华为云安全责任共担模型，明确了华为云与客户双方的安全责任边界，和各自应承担的安全责任。华为云的各云产品均会为客户提供包括帮助文档、使用手册、安全实施指南等，其中会包含安全使用的政策。
4-1-P-1-3 第三方供应商应遵守与其提供服务范围内所需遵守的法律法规。	4-1-P-1-3 第三方供应商应遵守与其提供服务范围内所需遵守的法律法规。	在华为云内部，华为云建立了正式的采购审核流程，在供应商入场前，华为云要求须同供应商签署合同、服务协议及保密协议。协议中包含对于双方的责任和义务、服务内容以及供应商的网络安全和隐私数据处理的要求，同时通过保密协议对违反保密性的条款进行了约束。此外，华为云已建立供应商选择和监督体系，并规范了研发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。
4-1-P-1-4 第三方供应商的风险管理和安全治理应作为一般网络安全风险管理和治理的一部分。	4-1-P-1-4 第三方供应商的风险管理和安全治理应作为一般网络安全风险管理和治理的一部分。	华为云网络安全与隐私保护管理要求中明确将供应商管理作为其总体网络安全管理与治理的主要领域之一。华为云建立了正式的采购审核流程，采购部门负责对供应商的资质进行评估，仅经过资质认证的供应商可以进入华为云的采购范围。此外，在供应商入场前，华为云要求须同供应商签署合同、服务协议及保密协议。合同与服务协议中明确了双方的责任和义务、服务内容及服务水平等要求，同时通过保密协议对违反保密性的条款进行了约束。华为云法务部门每年会对采购保密协议进行审阅及更新，以确保采购保密协议可以持续满足业务对供应商的管理要求。

7

华为云如何符合《CRF 网络安全监督框架》的要求

《CRF 网络安全监督框架》适用于获得 CST 许可或注册的组织（LSP），旨在提供信息和电信部门（ICT）的网络安全成熟度，为 LSP 提供了网络安全管理的通用原则及最佳实践。其中涵盖网络安全治理、资产管理、网络安全风险管理、逻辑安全及第三方安全五大领域。

以下内容将总结 CRF 中与云服务供应商相关的控制要求，并详细阐述了华为云作为客户的云服务供应商时，会如何帮助客户满足这些控制要求。

7.1 网络安全治理

“网络安全治理”要求客户建立适当的网络安全管理机制，涵盖网络安全战略、意识与培训、策略与程序、合规与审计等网络安全治理领域。相关控制要求及华为云的实践方式如下：

7.1.1 网络安全策略

定义网络安全战略并制定实施路线图，以实现战略的既定目标。

编号	具体控制要求	华为云的内部实践	客户的职责
1.1.1	<p>定义 [网络安全策略] 的要求，考虑以下方面：</p> <ul style="list-style-type: none">组织与网络安全相关的总体使命、目标和活动相关的法律法规合规要求建立网络安全项目最高管理层对	华为云制定了网络安全与隐私保护的管理要求，其中明确了华为云将构筑并全面实施端到端的网络安全体系作为重要战略，遵从业务所在地适用的法律法规，全面满足客户的网络安全需求。该战略得到公司最高管理层的批准。华为云建立并实施了文档化的网络安全政策和程序，为操作网络安全管理提供指导。网络安全政策和程序发布前需得到管理者审批。	客户应定义其网络安全战略，战略目标应符合相关法律法规的规定，明确实现网络战略应实施的网络安全项目，战略应得到组织负责人或代表的批准支持。

	网络安全的承诺		
1.1.2	确保[网络安全策略]得到最高管理层的批准。	该网络安全策略得到公司最高管理层的批准支持。	客户应确保网络安全策略得到最高管理层的批准。
1.1.3	在定义实施网络安全策略的[行动计划]时,请确保以下几点: •活动 •预算 •时间表 •资源(如能力、人员)	华为云在公司战略的指导下制定中长期的发展规划,支撑华为云业务的持续发展,并制定年度业务计划及实施路径图,其中包含网络安全相关活动、适用的法律法规的合规要求、开展和建立各类网络安全项目、支撑的人员及资源等,确保网络安全战略的有效落实。	客户应根据网络安全策略制定实施路径图或实施计划,明确落实网络安全战略所需的活动、支撑的人员及资源等,以确保网络安全策略的有效实施。
1.1.4	持续审查并根据要求更新[网络安全策略]和相应的[行动计划],特别是在相关立法和监管要求发生变化、重大组织变化或从以前的行动计划实施中吸取的教训的情况下。	华为云至少每年审查一次网络安全管理策略和网络安全计划,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。同时华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性,向最高管理层报告调查的结果和建议。	客户应根据计划的频率或外部监管的变化定期对网络安全策略进行审查和更新。

7.1.2 网络安全管理

定义并实施负责组织内网络安全活动的相关网络安全组织。

编号	具体控制要求	华为云的内部实践	客户的职责
1.2.1	定义[网络安全组织]的要求,考虑以下内容: • 网络安全委员会和分配代表组织内不同领域的成员 • 实施[行动计划]所需的网络安全职能/部门 • 分配角色和职责,确保明确区	在华为公司层面,全球网络安全与用户隐私保护团队 GSPC 作为最高网络安全管理机构,决策和批准公司总体网络安全战略。GSPO 及其办公室负责制定和执行华为端到端网络安全保障体系。华为云网络安全与用户隐私保护团队负责制定华为云安全策略,并定期对策略的执行情况进行定期审视,确保安全治理的策略、规范和具体措施在各业务领域的流程落地,实现端到端的安全治理。同时,华为云在各产品、	客户应在组织内建立专门的网络安全职能,定义网络安全组织架构以及角色与职责,确保各职责间没有利益冲突,明确网络安全职能部门应落实网络安全计划的各项活动。

	分相互冲突的职责和职责范围。	服务的业务团队中明确规定了所有员工对应角色的网络安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的安全管理职责。网络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。华为云遵循职责分离和权限制衡原则，对不相容职责进行分离，实现合理的权限分工，同时制定了 SOD 权责分离管理矩阵以帮助实现该管理原则。	
1.2.2	实施定义的[网络安全组织]。	在华为公司层面，全球网络安全与用户隐私保护团队 GSPC 作为最高网络安全管理机构，决策和批准公司总体网络安全战略。GSPO 及其办公室负责制定和执行华为端到端网络安全保障体系。华为云网络安全与用户隐私保护团队负责制定华为云安全策略，并定期对策略的执行情况进行定期审视，确保安全治理的策略、规范和具体措施在各业务领域的流程落地，实现端到端的安全治理。沙特网络安全与隐私保护官遵循公司最高层面的网络安全战略，并在沙特执行落地。	客户应在组织内建立专门的网络安全职能。
1.2.3	通过定义的[网络安全组织]实施 [行动计划]。	在华为公司层面，全球网络安全与用户隐私保护团队 GSPC 作为最高网络安全管理机构，决策和批准公司总体网络安全战略。全球网络安全与用户隐私保护官 GSPO 及其办公室负责制定和执行华为端到端网络安全保障体系。华为云网络安全与用户隐私保护团队负责制定华为云安全策略，并定期对策略的执行情况进行定期审视，确保安全治理的策略、规范和具体措施在各业务领域的流程落地，并确保网络安全计划中的各项活动有效的开展，实现端到端的安全治理。	客户应明确网络安全职能部门须落实网络安全计划的各项活动。
1.2.4	通过监测、处理冲突和实施必要的改进措施，监督网络安全委员会[行动计划]的实施。	华为云网络安全团队根据建立的网络安全项目和计划或风险评估的结果，制定必要的改进措施并管理和推动各业务部门对各程序计划的有效执行。此外，华为云至少每年审查一次网络安全管理策略和网络安全计划，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。	客户应通过监测、处理冲突和实施必要的改进措施，监督网络安全职能部门对网络安全计划中各项活动的实施。

		况。同时华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性，向最高管理层报告调查的结果和建议。	
--	--	--	--

7.1.3 网络安全合规

确保其符合内部和相关外部（国家、国际）监管要求。

编号	具体控制要求	华为云的内部实践	客户的职责
1.3.1	定义[网络安全合规要求]，考虑以下因素： <ul style="list-style-type: none">• 与网络安全相关的国家立法和监管要求• 本地认可的国际/跨境要求（例如包含在国际协议或承诺中）• 组织的内部要求	华为云在其网络安全策略中明确合规流程，定期识别和记录合规要求。同时，华为云设立了专岗同外部各方保持积极的联系，以追踪法律、法规、国际标准等相关要求变化。	客户应定期识别并遵守相关国家的网络安全法律法规、国家批准的国际协议和与网络安全相关的要求。
1.3.2	定义{合规流程}以确保定期识别、记录和传达合规要求（例如，当新的监管要求生效时，有必要更新组织的网络安全要求）。	华为云在其网络安全策略中明确合规流程，定期识别和记录合规要求，当识别到与华为云服务相关的法律、法规，华为云将及时调整内部安全要求和安全控制水平，跟进对法律、法规要求的符合性。	客户应确保定期识别、记录和传达合规要求。
1.3.3	确保合规性要求纳入组织内部。	当识别到与华为云服务相关的法律、法规，华为云将及时调整内部安全要求和安全控制水平，跟进对法律、法规要求的符合性。	客户应确保将合规要求纳入组织内部的管理要求中。
1.3.4	通过使用专用工具（如 GRC 工具）自动化合规活动。	华为云使用 Compss 自动化合规评估和安全治理平台，将全球多个国家地区的安全要求作为输入，形成自动化合规策略，对云上多个服务进行自动化扫描，同时华为云使用风险管理平台对风险进行自动跟踪与监控。	客户可使用专用工具进行自动化合规活动。 华为云安全治理云图（Compliance Compass）是一个自动化合规评估和安全治理的平

			台，以华为内部“云服务网络安全与合规标准”(Cloud Service Cybersecurity & Compliance Standard, 3CS)为基座，将华为积累的全球安全合规经验服务化，开放 PCI DSS、ISO27701、ISO27001 等安全治理模板，将合规语言 IT 化实现自动化扫描，可视化呈现合规状态，一键生成合规遵从性报告，帮助客户快速实现云上业务的安全遵从，提升租户获得法规及行业标准认证的效率。
1.3.5	持续审查和优化[网络安全合规要求]以及流程的有效性，以确保合规。	华为云每年会对建立的网络安全合规相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对网络安全合规要求以及流程的有效性进行审查和优化。

7.1.4 网络安全审计

定期进行涵盖内部和外部合规要求的独立网络安全审计，以衡量组织的合规水平。

编号	具体控制要求	华为云的内部实践	客户的职责
1.4.1	定义[网络安全审计要求]，考虑以下因素： <ul style="list-style-type: none">进行定期审计（例如，每年至少对关键系统进行一次审计）	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。同时华为云有专门的审计团队定期评估策略、规程及配套措施和	客户应每年至少对关键系统进行一次审计，保留和保护审计记录，将审计结果和建议向管理层报告，以确定网络安全控制的合

	<ul style="list-style-type: none"> • 保护和保留[审计记录] • 向最高管理层报告 	指标的符合性和有效性，向最高管理层报告调查的结果和建议，同时保留审计记录免受未经授权的访问。	规性和有效性。
1.4.2	定义并执行{内部审计}流程，以验证是否符合已确定的 [网络安全合规要求]。	华为云制定了内审管理流程，规范内部审计原则、审计管理流程和审计频率。华为云每年由专门的审计团队执行一次内部审计工作，以检查公司内部控制体系的运行情况，评估策略、规程及配套措施和指标的符合性和有效性。	客户应定期由组织内负责网络安全的职能部门进行内部审核，以确定网络安全控制的合规性和有效性。
1.4.3	记录调查结果和建议并将其提交给最高管理层。	华为云会向最高管理层报告调查的结果和建议。管理层进行审阅并对整改情况进行跟进。	客户应将审计结果和建议提交至组织的最高管理层。
1.4.4	保护 [审计记录] 免受未经授权的访问、修改和破坏。	华为云制定了数据安全策略及数据安全保护管理规定，采取适当保护措施并严格执行，以保证审计记录安全。华为云通过限制访问权限的方式来保护审计记录免受非授权的访问、修改和删除。	客户应保护审计记录免受未经授权的访问、修改和破坏。
1.4.5	确保保留审计记录作为证据，例如遵守法律和监管要求。	华为云根据法律、法规、规章、合同和业务要求，对审计记录进行保留，以证明其合规性。	客户应确保保留审计记录作为其遵守法律法规及监管的证据。
1.4.6	持续审查和优化 [网络安全审计要求]以及开展审计和审查活动流程的有效性。	华为云每年会对建立的网络安全审计相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对网络安全审计以及流程的有效性进行审查和优化。

7.1.5 网络安全意识&培训

定期进行网络安全意识和培训，以确保其人员具备履行职责所需的资格和技能。

编号	具体控制要求	华为云的内部实践	客户的职责
1.5.1	定义[网络安全意识和培训要求]，考虑以下因素： <ul style="list-style-type: none"> • 目标和范围 	华为云建立了培训机制，以提高员工的信息安全意识，根据不同的角色、岗位为员工设计合适的培训方案，其中一般员工的培训频率为至少每年一次，核心岗位员工培训频	客户应制定完善的安全意识和技能培训管理机制，根据培训对象的职能和角色

	<ul style="list-style-type: none">• 培训次数和频率/年• 分配的资源	率更高。此外，华为云制定了专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。	来制定培训内容，定期分析并更新培训内容。
1.5.2	<p>定义并实施[网络安全意识和培训计划]（例如，定义目标、范围、目标受众、验证标准），其中包括各种网络安全主题，并考虑以下内容：</p> <ul style="list-style-type: none">• 目标受众的网络安全角色和责任• 网络安全事件和威胁趋势（例如电话诈骗和冒充电话等社会工程攻击）• 建议人员不要尝试未经授权的活动（例如，在系统上引入或使用未经授权的设备或软件，未经适当授权定位设备）• 安全处理便携式设备和存储媒体、电子邮件服务（尤其是垃圾邮件和网络钓鱼电子邮件）、互联网冲浪服务和社交媒体	华为云为确保员工的信息安全意识能够符合公司要求建立了一系列的网络安全培训及学习机制，要求员工持续学习网络安全知识，了解相关的政策和制度，会涵盖安全处理钓鱼邮件、移动设备和存储介质的安全处理、安全的互联网浏览及安全使用社交媒体等主题。面向全员开展形式多样的网络安全宣传活动，包括网络安全社区运营、网络安全典型案例宣传、网络安全活动周、网络安全动画宣传片等，以提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营。	客户制定的网络安全意识计划应涵盖最新的网络威胁及如何防范这些威胁。
1.5.3	加强并实施[网络安全意识和培训要求]，定期进行验证测试，以评估所进行的意识与培训计划的有效性并记录评估结果（例如检查人员是否会点击	新员工在入职后均须参加公司组织的网络安全考试，员工仅能在考试通过后才可以正式转正。针对在职员工，华为公司将网络安全纳入员工行为准则，通过公司统一开展的年度例行学习、考试和绩效考核措施，每半年对内部员工开展一次绩效考核，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	客户应定期进行验证测试，以评估所进行的意识与培训计划的有效性并记录评估结果。

	电子邮件中的可疑链接)。	意识。	
1.5.4	加强并实施[网络安全意识和培训要求],以确定在何种情况下必须提供[网络安全意识和培训计划](例如,对新用户的初始网络安全培训、信息系统或工作角色变更后的培训)。	新员工在入职后均须参加公司组织的网络安全考试,员工仅能在考试通过后才可以正式转正。针对在职员工,华为云每年定期组织信息安全意识培训、信息安全知识宣传。在员工在职期间持续对员工的安全意识教育进行培训,培养员工安全意识,以提升全员的网络安全意识,规避网络安全违规风险,保证业务的正常运营。	客户应明确在何种情况下对员工进行安全意识教育培训。
1.5.5	根据以下人员,调整[网络安全意识和培训计划],为目标人群提供专业或安全相关技能和培训: •网络安全全部人员 •从事软件开发的人员 •参与网络安全风险管理部门的人员 •有权访问关键信息资产的人员 •执行人员	华为云建立了自己的培训机制,根据不同的角色、岗位为员工设计合适的培训方案。其中一般员工的培训频率为至少每年一次,核心岗位员工培训频率更高。华为云对开发人员、运维工程师及网络安全管理人员等重点岗位实施专项管理,包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。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。	客户应向直接从事与网络安全相关的人员提供必要的和定制的培训和专业技能组合。
1.5.6	持续审查并优化[网络安全意识和培训要求]以及[网络安全意识和培训计划]。	华为云每年会对建立的人员意识培训计划进行审阅和更新,同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视,确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对网络安全意识和培训的要求以及流程的有效性进行审查和优化。

7.1.6 项目管理中的网络安全

确保应用的项目管理方法中包含组织定义的网络安全要求。

编号	具体控制要求	华为云的内部实践	客户的职责
1.7.1	定义[项目管理中的网络安全要	华为云在项目管理中将安全目标纳入项目目标,在项目初期对其进行	客户应将网络安全要求融入项目

	<p>求], 考虑以下因素:</p> <ul style="list-style-type: none"> • 定义网络安全在项目管理中的整合(例如, 网络安全人员作为项目团队的一部分) • 定义项目目标以确保网络安全包含在项目的所有阶段 	<p>网络安全风险评估并在整个项目交付过程中定期评审网络安全影响。</p>	<p>管理中, 确保在项目管理中对识别的网络安全风险进行管理。</p>
1.7.2	根据[风险评估要求]在每个项目开始和过程中进行风险评估, 以识别网络安全风险(如有), 并确定缓解计划。	在项目初期对其进行信息安全风险评估并在整个项目交付过程中定期评审信息安全影响。以确保对组织的运行和安全没有负面影响, 若识别到网络安全风险, 将对评估进行正式记录并制定风险处置计划, 网络安全与用户隐私团队对风险处置跟进过程进行定期评审, 确保符合公司风险管理要求。	客户应在项目开始和过程中进行风险评估, 以识别网络安全风险, 并确定缓解计划。
1.7.3	在项目过程中跟踪已识别的网络安全风险并监控缓解计划的实施。[网络安全风险处理和监控]。	华为云各业务团队根据要求定期执行信息安全风险评估。网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议, 识别有关的网络安全风险, 并对风险处置跟进过程进行定期评审, 确保符合公司风险管理要求。风险评估报告完成后由高级管理层进行审批。	客户应定期在项目过程中跟踪已识别的网络安全风险并监控缓解计划的实施。
1.7.4	持续审查和优化[项目管理中的网络安全要求]。	华为云每年会对建立的安全开发、安全测试、配置管理等相关规范和策略流程进行审阅和更新, 同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视, 确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对项目管理中的安全要求进行审查和更新。

7.1.7 人力资源中的网络安全

确保人力资源相关的网络安全要求在其工作关系发生任何变化时得到满足。

编号	具体控制要求	华为云的内部实践	客户的职责

1.8.1	定义[人力资源网络安全要求], 考虑以下因素:		
	定义与组织内人员（包括承包商）相关的网络安全要求，包括雇佣前、工作期间以及工作完成/终止后。	华为云建立了人员信息安全管理规定，明确了华为云各类员工分层分级的信息安全管理要求，对内外部员工从雇佣前、在职期间及离职后各阶段的安全管理进行了规范，明确了员工应遵循的华为云网络安全职责。	客户应制定并落实员工在雇佣前、雇佣期间及雇佣后的网络安全要求。
	对所有求职者进行背景核查。	人员任用前，华为云通过既定的新进员工背景调查机制对满足特定条件的拟聘员工进行背景审查，同时，在适用法律允许的情况下，华为云会根据可接触的资产的机密性，在聘用员工或外部人员前对其进行背景调查。	客户应在雇佣前对所有职位的候选人进行背景调查进行筛选和审查。
	聘请高度专业的人员从事与关键系统相关的工作。	华为的安全技术团队包括全球各地业界优秀的信息安全、产品安全、应用安全、系统安全、网络安全、云服务安全、运维运营安全、隐私保护等方面专家。同时，华为云对运维工程师等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。	客户应聘请高度专业的人员从事与关键系统相关的工作。
	确保与雇佣相关的条款和协议也涵盖行为准则（例如保密协议、网络安全责任），并在与组织的雇佣关系期间和之后被包括在内。	员工与公司签署的聘用协议中包含保密条款，其中明确说明员工的网络安全责任，以确保在入职前对应遵循的保密条款进行确认。华为云规定员工离职时需签署离职保密承诺书，确认其应持续承担的信息安全责任及职责。	客户应在劳动合同及保密条款中包含人员应遵守的网络安全的要求。
	确保所有人员签署行为准则。	华为云将网络安全纳入华为员工商业行为准则，通过公司统一开展的年度例行学习、考试和签署活动来传递公司对全员在网络安全领域的责任，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。	客户应确保所有人员签署行为准则。
	执行[信息资产的可接受使用]。	华为云已制定并实施资产的使用规则，包括管理原则、相关人员职责、办公计算机安全要求、办公网	客户应定义定资产的可接受使用规则，包括但不

		络安全要求、办公应用系统安全要求、存储介质与端口安全要求、办公外设安全要求、非华为计算机安全要求以及相关违规的处罚等。	限于办公终端的安全使用规范、存储介质的安全要求、办公网络的安全使用规范等。
1.8.2	确保当个人被重新分配或转移到组织内的其他职位时，执行必要的行动（例如，根据新的运营角色修改访问授权）。	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。	客户应确保在员工职位变更时对其相关权限和资产进行审查和变更。
1.8.3	对不符合组织网络安全要求的人员实施纪律处分。	华为建立了严密的安全责任体系，贯彻违规问责机制。华为云以行为和结果为主要依据对员工进行问责。根据华为云员工安全违规的性质，以及造成的后果确定问责处理等级，分级处理。对触犯法律法规，移送司法机关处理。直接管理者和间接管理者存在管理不力或知情不作为的，须承担管理责任。违规事件处理根据违规个人态度与调查配合情况予以加重或减轻处理。华为云的违规政策供所有员工进行查看学习，并定期组织培训提升员工对违规行为、违规后果、惩罚措施的了解。	客户应对不符合组织网络安全要求的人员实施纪律处分。
1.8.4	确保在员工完成/终止组织内的专业服务后，已采取必要的措施（例如，撤销员工访问权限和特权、检索分配的信息资产、保留对以前由被终止人员控制的信息资产的访问权）。	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，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。华为云规定员工离职时需签署离职保密承诺书，确认其应持续承担的信息安全责任及职责。	客户应确保在员工离职后对其相关权限和资产进行审查和回收。
1.8.5	持续审查和优化	华为云每年会对建立的人员信息安全安	客户应根据计划

	[人力资源网络安全要求]以及相关流程的有效性。	全相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	的频率定期对人员网络安全管理要求以及流程的有效性进行审查和优化。
--	-------------------------	---	----------------------------------

7.2 资产管理

“资产管理”要求客户从资产的生命周期的维度建立适当的资产安全管理机制，覆盖资产的发现、资产分类、资产的使用、资产的维护及资产处置。控制要求及华为云的实践方式如下：

7.2.1 资产发现

维护所有信息资产的最新资产清单，其中包括所有相关细节以促进信息资产的有效保护。

编号	具体控制要求	华为云的内部实践	客户的职责
2.1.1	定义[资产发现要求]考虑以下事项： <ul style="list-style-type: none">• 定义信息资产清单[资产清单]（例如软件、硬件、信息、关键信息资产、设备、数据库）• 定义更新[资产清单]的频率• 信息资产的所有权	华为云制定了资产管理程序，明确了信息资产的分级定级办法以及针对各类资产应遵循的授权规则。华为云对信息资产进行分类并由专门的工具进行监控和管理，形成资产清单，并明确了资产所有者。	客户应明确资产发现要求，编制和维护资产清单。
2.1.2	定义并实施{资产发现}流程以识别（例如资产发现工具）属于组织的所有信息资产并更新[资产清单]。为每个信息资产分配一个资产所有者。	华为云通过 CAM 资产管理系统实时监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理。此外，华为云设置配置经理对所有业务单元进行配置管理，资源配置模型分为主机、服务树、云基础设施和网络设备，通过构建配置项映射和资源生命周期管理，支撑现网运维获得的稳定和安全，并通过专业的配置管理数据库工具（CMDB）对配置	客户应遵循已建立的资产发现流程，编制和维护资产清单，对不同类别的资产采取适用的保护措施。 华为云的企业主机安全（Host Security Service，简称 HSS）为客

		项、配置项的属性和配置项之间的关系进行管理。	户提供统一的管理界面，供客户查询并管理云服务，是服务器的贴身安全管家，为客户提供资产管理功能，包括提供账号、端口、进程、Web 目录和软件等安全资产信息的管理和分析。
2.1.3	根据要求中定义的频率或信息资产发生修改时（即资产的添加和移除），审查并更新[资产清单]。	华为云通过 CAM 资产管理系统实时对资产管理平台中记录的信息资产的添加或移除进行监控和更新维护。此外，华为云设置配置经理对所有业务单元进行配置管理，资源配置模型分为主机、服务树、云基础设施和网络设备，通过构建配置项映射和资源生命周期管理，支撑现网运维获得的稳定和安全，并通过专业的配置管理数据库工具（CMDB）对配置项、配置项的属性和配置项之间的关系进行管理。	客户应遵循资产发现流程中规定的频率或资产发生变更时，对资产清单进行更新维护。华为云的企业主机安全（Host Security Service, 简称 HSS）的资产管理功能可深度扫描出主机中的账号、端口、进程、Web 目录、软件信息和自启动任务，供客户查询并管理云服务。
2.1.4	使用专用的自动化工具来发现信息资产。整合信息资产，并从中央系统对其进行跟踪。	华为云通过 CAM 资产管理系统实时监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理。此外，华为云利用自动化工具采集物理机、虚拟机、容器、网络设备等组件基础配置信息，如规格、OS 相关配置，该工具与配置管理数据库工具（CMDB）对接，将配置信息上报到 CMDB，从而确保数据的准确性。	客户应使用专用的自动化工具来发现信息资产，并进行跟踪。华为云的企业主机安全（Host Security Service, 简称 HSS）的资产管理功能可以统一管理主机中的信息资产，包括账号、端口、进程、Web 目录和软件等安全资产信息的管理和分析。

2.1.5	不断审查和优化 [资产发现要求] 和{资产发现}流程。	华为云每年会对建立的资产发现流程与要求进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对资产发现要求以及流程的有效性进行审查和优化。
-------	-----------------------------	--	-------------------------------------

7.2.2 资产分类

对信息资产进行分类，以确保对信息资产进行基于风险的保护。

编号	具体控制要求	华为云的内部实践	客户的职责
2.2.1	定义[资产分类要求]考虑以下事项： •信息资产的分类和标签以及识别、处理、转移、存储、返还、删除和处置的相应保护措施	华为云制定了资产管理程序，明确了信息资产的分级定级办法以及针对各类资产应遵循的授权规则。华为云对信息资产进行分类并由专门的工具进行监控和管理。对于不同类别的信息资产，制定了涵盖资产全生命周期（包括识别、处理、转移、存储、返还、删除和处置）各环节的保护措施。	客户应建立正式的资产管理程序，对其资产进行分类。
2.2.2	定义并实施{资产分类}流程，根据特定标准（例如关键性、商业价值、法律要求、机密性、完整性和可用性）和 [信息保护要求] 对 [资产清单] 中的信息资产进行分类和标记。	华为云通过 CAM 资产管理系统实施监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理，并形成资产清单为每个资产均被指定所有者。此外，华为云设置配置经理对所有业务单元进行配置管理，资源配置模型分为主机、服务树、云基础设施和网络设备，通过构建配置项映射和资源生命周期管理，支撑现网运维获得的稳定和安全，并通过专业的配置管理数据库工具（CMDB）对配置项、配置项的属性和配置项之间的关系进行管理。华为云对数据进行分级管理，结合机密性、完整性、可用性、合规性进行综合定级，将数据分为多个安全级别并分别给出该级别数据的定义。同时规定了不同级别数据的安全实施要求、稽查要求以及应急响应及演练要求。各业务领域遵照数据定级标准对其领域内数据标记安全等级。	客户应依照法律要求、资产价值、资产对组织的重要性和敏感性标注相应资产的分类。

2.2.3	按照{资产分类}流程处理资产。	华为云制定了资产管理程序，明确了信息资产的分级定级办法以及针对各类资产应遵循的授权规则，同时也建立了信息资产保密管理要求，明确华为云对各级别信息资产应采取的保密措施，规范使用资产的行为，使公司资产得到合理保护和共享，确保资产按照其对组织的重要程度受到适当水平的保护。	客户应依据不同级别的资产分类定义和制定信息和技术资产管理的网络安全要求，确保资产获得适当水平的保护。
2.2.4	持续审查并优化 [资产分类要求]{资产分类}流程。	华为云每年会对建立的资产分级分类要求进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对资产分级分类要求以及流程的有效性进行审查和优化。

7.2.3 自带设备

管理出于业务目的使用的员工设备，以保护组织免受此类设备带来的风险。

编号	具体控制要求	华为云的内部实践	客户的职责
2.3.1	在组织内定义 [BYOD 的网络安全要求]，考虑以下因素： <ul style="list-style-type: none">• 将个人信息与业务信息隔离• 根据组织的商业利益限制使用设备• 访问关键系统	华为云制定了移动设备管理规定，以实施对移动计算设备的统一管理。对移动设备使用的原则、职责、权限要求、设备管理安全要求、网络接入要求及违规处罚等均做出规定。其中明确将个人信息与业务信息进行隔离，并要求 BYOD 上的组织数据和信息不涉及华为的核心信息资产，同时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，并按照员工权限对应用程序的访问范围进行控制。	客户应制定移动设备安全和 BYOD 管理策略，根据设备使用者的工作角色和权限管理和限制对移动设备的使用。
2.3.2	在组织内执行定义的 [BYOD 的网络安全要求]。	华为云员工遵循华为云移动设备管理规定，履行规范中针对移动设备使用的安全要求，保障移动办公终端上的公司数据的信息安全，对资产的使用负责。	客户应遵循已定义的移动设备和 BYOD 的安全管理策略，保障移动设备上数据的安全性。
2.3.3	确保存储在设备上的组织信息已加密。	华为云建立了保护技术设备上的数据的加密策略与密钥管理机制，对人员的权限与职责分配、加密级	客户应确保对存储在设备中的数据和信息资产进

		别、加密方法进行了规定。同时，针对不同级别的数据，限制含有涉密数据的电子流或邮件发布到移动 BYOD 端的应用中，BYOD 上的组织数据和信息不涉及华为的核心信息资产。	行加密措施。
2.3.4	持续审查和优化组织内的 [BYOD 的网络安全要求]。	华为云每年会对建立的移动办公终端相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对移动设备和 BYOD 的安全要求进行审查和更新。

7.2.4 可接受的使用策略

定义和实施可接受的使用策略，以保护组织免受信息资产不当使用所带来的风险。

编号	具体控制要求	华为云的内部实践	客户的职责
2.4.1	定义[可接受的信息资产使用]的要求，考虑以下事项： •信息资产的可接受使用（例如，仅在获得定义角色（如相关 IT 部门）的正式批准后安装软件或硬件）	华为云已制定并实施资产的使用规则，包括管理原则、相关人员职责、办公计算机安全要求、办公网络安全要求、办公应用系统安全要求、存储介质与端口安全要求、办公外设安全要求、非华为计算机安全要求以及相关违规的处罚等。此外，华为云制定并实施桌面终端服务软件标准及开源软件清单，仅可以使用其中定义的标准操作系统和软件应用程序。在终端设备上的 iDesk 程序设有上审阅后的应用程序白名单，华为云内部办公软件仅能从该平台进行下载。	客户应定义定资产的可接受使用规则，包括但不限于办公终端的安全使用规范、存储介质的安全要求、办公网络的安全使用规范等。
2.4.2	确保组织内人员已实施[可接受的信息资产使用]（例如，禁止安装不需要的软件和应用程序，控制对网页的访问，禁止访问恶意网站或危险网站）。	华为云实施资产的使用规则，要求组织内的人员遵循资产的可接受信息资产的使用要求。遵守办公计算机安全要求、办公网络安全要求、办公应用系统安全要求、存储介质与端口安全要求、办公外设安全要求、非华为计算机安全要求以及相关违规的处罚等。	客户应确保员工遵循已制定的资产的可接受使用规则，对办公终端、存储介质、办公网络等资产实施安全管理措施。
2.4.3	持续审查并优化[可接受的信息资产使用]	华为云每年会对建立的资产的安全使用相关规范和策略流程进行审阅	客户应根据计划的频率定期对资产的安全使用相关规范和策略流程进行审阅

	产使用]的要求。	和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	产的安全使用要求进行审查和更新。
--	----------	---	------------------

7.2.5 资产维护

维护信息资产并在发生网络安全事件时将其恢复，以确保其持续可用性和完整性。

编号	具体控制要求	华为云的内部实践	客户的职责
2.5.1	定义[资产维护要求]，考虑以下因素： <ul style="list-style-type: none">• 资产维护• 跟踪和监控• 恢复计划	华为云制定了资产安全管理要求，涵盖虚拟机、IP、域名、密钥和证书等多类信息资产的全生命周期管理规范。同时，对于硬件资产，华为云建立了数据中心运维管理相关的制度与流程，明确了对设备的具体管控措施以及需要例行实施的维护计划等。	客户应定义资产维护要求，明确对资产的跟踪与监控以及资产的恢复流程。
2.5.2	定义并实施{资产维护}流程，以维护和修复组织的信息资产（包括场外资产），并记录这些活动。	对于硬件资产，华为云建立了数据中心运维管理相关的制度与流程，明确了对设备的具体管控措施以及需要例行实施的维护计划等。同时，华为云通过 CAM 资产管理系统实时监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理。	客户应实施资产维护流程，以维护和修复组织的信息资产。
2.5.3	根据组织定义的恢复计划，在安全事件期间或之后执行资产恢复。	华为云根据内部业务连续性管理体系的要求，为支撑云服务持续运行的关键业务制定了完善的恢复策略。恢复策略涵盖备用场地、设备、人员、信息系统、第三方等各个方面，确保业务能在恢复时间目标内恢复到可接受水平。	客户应确保能够在发生网络安全事件后快速恢复资产。
2.5.4	对信息资产进行远程监控和跟踪（例如，使用位置跟踪技术），并确保信息资产保存在组织控制的区域内。	华为云通过 CAM 资产管理系统实时监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理。同时，华为云制定并实施办公场所安全管理规定，对员工的安全责任与行为规范提出要求，确保无人值守的用户设备有适当的保护。此外，华为云制定并实施办公计算机安全管理规定，明确办公资产使用人有义务确保所使用资产的安全，并对使用状	客户应对信息资产进行监控和跟踪，确保信息资产保存在组织控制的区域内。

		况负责。员工携带办公便携机外出时将其随身携带或妥善存放，确保便携机中所存储华为信息的安全。如办公计算机丢失或被盗，员工将及时报告。	
2.5.5	持续审查和优化 [资产维护要求] 和{资产维护}流程。	华为云每年会对建立的资产维护流程与要求进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对资产维护要求以及流程的有效性进行审查和优化。

7.2.6 资产的安全处置

确保信息资产的安全处置，以防止未经授权披露或修改存储在处置资产上的信息。

编号	具体控制要求	华为云的内部实践	客户的职责
2.6.1	定义[资产处置要求]，考虑以下事项： •根据[资产清单]中定义的信息资产分类和标签，制定信息资产处置规则	华为云制定了资产管理程序，明确了信息资产的分级定级办法以及针对各类资产应遵循的授权规则，同时也建立了信息资产保密管理要求，明确华为云对各级别信息资产应采取的保密措施，规范使用资产的行为，使公司资产得到合理保护和共享，确保资产按照其对组织的重要程度受到适当水平的保护。华为云通过 CAM 资产管理系统实施监控资产管理平台中记录的信息资产的盘存和维护状况，对信息资产进行分类、监控和管理。	客户应依据不同级别的资产分类定义和制定信息和技术资产管理的网络安全要求，确保资产按照其对组织的重要程度受到适当水平的保护。
2.6.2	根据[资产处置要求]，定义并实施{资产处置}流程来处理信息资产的处置。在不再需要（或重复使用）时使用适当的技术（例如安全擦除、钻孔、切碎），以防止未经授权披露或修改存储在资产上的信息。	对于存储公司信息的存储介质资产，华为云制定并实施介质管理规定，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，并对销毁操作进行记录。存储公司保密信息的存储介质报废时由专人确保其上存储的信息均被清除且不可恢复，处理方式包括消磁、物理销毁或低级格式化。	客户应定义并实施资产处置流程来处理信息资产的处置，以防止未经授权的披露或修改。

2.6.3	持续审查和优化 [资产处置要求] 和{资产处置}流程。	华为云每年会对建立的资产处置流程与要求进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对资产处置要求以及流程的有效性进行审查和优化。
-------	-----------------------------	--	-------------------------------------

7.3 网络安全风险管理

“网络安全风险管理”要求客户以系统性方法管理网络安全风险，并按照组织政策、程序及相关法律法规保护组织的信息资产。控制要求及华为云的实践方式如下：

7.3.1 网络安全风险评估

建立并实施适当的网络安全风险评估方法来识别、分析和评估风险以保护信息资产。

编号	具体控制要求	华为云的内部实践	客户的职责
3.1.1	定义[网络安全风险评估要求]，考虑以下因素： <ul style="list-style-type: none">• 组织中风险评估的目的和范围• 应在组织中进行风险评估的频率和条件• 确保[网络安全风险评估要求]涵盖组织、个人、其他组织以及与组织信息系统相关的国家的信息资产和服务的风险	华为云建立了信息安全风险管理规范，明确风险管理应遵循的关键流程、风险管理范围、风险管理相关责任部门及风险管理中应遵循的标准，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断。华为云各业务团队根据要求定期执行信息安全风险评估。	客户应根据资产的机密性、完整性和可用性，建立符合其组织战略的网络安全风险管理的方法和程序。
3.1.2	定义并实施{风险评估}流程，其中包括： <ul style="list-style-type: none">• 风险识别：根据组织的信息资产[资产发现]识别并记录内部和外部风险。在[风险登记册]中维护	华为云各业务团队根据要求定期执行信息安全风险评估，网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，识别有关的网络安全风险，并对风险处置跟进过程进行定期评审，确保符合公司风险管理要求。风险评估报告完成后由高级管理层进行审批。风险评估的主要流程如	客户应遵循网络安全风险评估的流程，对组织的资产进行内外部风险的识别，并将已识别的风险记录在风险登记册中，根据风险发生的概率和影

	<p>已识别的风险</p> <ul style="list-style-type: none"> 风险分析：根据概率和影响分析和记录已识别的风险 风险评估：根据组织的风险偏好，识别、确定优先级并记录应处理或接受的风险。风险评估结果必须得到最高管理层的正式批准 根据要求，向CST报告[风险登记册]中的主要网络安全风险以及补救计划 	<p>下：</p> <ul style="list-style-type: none"> 风险管理人员认别各业务场景中所涉及的固有风险，基于华为云面临的威胁和脆弱性进行风险评估； 基于固有风险清单，结合已有的风险管控措施，输出残余风险清单，并将风险及时录入风险管理平台，包括风险描述、所属领域、风险等级、风险来源等； 基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划。风险评估报告完成后由高级管理层进行审批。 <p>华为云为配合客户向CST报告主要的网络安全风险以及补救计划，华为云会遵从与客户订的协议中约定的要求，会安排专人积极配合客户的需求。</p>	响程度对风险进行分析，同时根据组织的风险偏好，确定风险优先级并记录应处理或接受的风险，并将主要的风险及补救计划与CST报告。
3.1.3	<p>将{风险评估}流程集成到LSP风险管理中，并至少将其应用于以下事件：</p> <ul style="list-style-type: none"> 在重大技术项目或组织或技术架构发生重大变化的早期阶段 在向市场推出新产品和服务之前 	<p>在项目初期对其进行信息安全风险评估并在整个项目交付过程中定期评审信息安全影响。同时，华为云制定了变更管理的管理规定和变更流程，各项变更均需通过多个环节的审核，以确保对组织的运行和安全没有负面影响。</p>	客户应确保在技术项目的早期阶段，技术基础设施发生重大更改之前，或新的技术服务和产品的规划阶段和上线之前开展网络安全风险评估，以保证组织信息安全的持续运行。
3.1.4	通过使用专用工具（如GRC工具）自动化风险评估活动。	华为云使用Compss自动合规评估和安全治理平台，将全球多个国家地区的安全要求作为输入，形成自动化合规策略，对云上多个服务进行自动化扫描实施风险评估活动，同时华为云使用风险管理平台对风险进行自动跟踪与监控。	客户应使用专用的工具自动化风险评估活动。
3.1.5	持续审查和优化[网络安全风险评估要求]。	华为云每年会对建立的网络安全风险评估要求进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流	客户应根据计划的频率定期对网络安全风险管理相关的要求进行审查和更新。

		程落地。	
--	--	------	--

7.3.2 网络安全风险处置与监控

建立并实施适当的网络安全风险处理和监控方法，以管理已识别的风险并监控处理计划。

编号	具体控制要求	华为云的内部实践	客户的职责
3.2.1	定义[网络安全风险处置和监控的要求]，考虑以下内容： <ul style="list-style-type: none">• 风险处置计划• 风险监控计划	华为云制定了信息安全风险评估方法，识别华为云的威胁和漏洞，基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划，并对风险处置计划的实施进行监控。	客户应定义网络安全风险处置和监控计划，对识别的风险进行处置和监控。
3.2.2	定义并实施{风险处理}流程，描述如何处置评估的风险，从而产生[风险处置计划]。	华为云各业务团队根据要求定期执行信息安全风险评估，基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划。同时，网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，识别有关的网络安全风险，并对风险处置跟进过程进行定期评审，确保符合公司风险管理要求。	客户定义并实施风险处理流程，识别可能存在的网络安全风险，并制定风险处置计划。
3.2.3	定义并实施{风险监控}流程，包括已定义的风险监控计划、定期监控风险处置计划的实施情况、风险处理后的剩余风险以及已接受风险的状态。	网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，识别有关的网络安全风险，并对风险处置跟进过程进行定期评审。此外，华为云为确保风险管控的有效性并实现持续改进，需定期对风险度量指标进行持续监控，根据度量值管控失效的风险，并纳入风险管理进行持续处置。	客户应定期对已制定的风险处置计划的实施情况进行监控，识别风险处理后的剩余风险以及已接受风险的状态。
3.2.4	通过使用专用工具（如 GRC 工具）自动化风险处置和监控活动。	华为云使用 Compss 自动化合规评估和安全治理平台，将全球多个国家地区的安全要求作为输入，形成自动化合规策略，对云上多个服务进行自动化扫描实施风险评估活动，同时华为云使用风险管理平台对风险进行自动跟踪与监控。	客户应使用专用的工具自动化风险处置和监控活动。
3.2.5	持续审查和优化	华为云每年会对建立的网络安全风	客户应根据计划

	[网络安全风险处置和监控要求]。	险评估要求进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	的频率定期对网络安全风险管理相关的要求进行审查和更新。
--	------------------	--	-----------------------------

7.4 逻辑安全

“逻辑安全”中要求客户制定网络安全运营和安全管理的策略及流程，包括变更管理、身份与访问管理、漏洞与补丁管理、密码管理、备份与恢复、网络安全事件管理等方面。相关控制要求及华为云的实践方式如下：

7.4.1 密码学

确保有效和充分地使用密码学，为传输、静止和使用中的信息提供机密性、完整性、身份验证和不可否认性。

编号	具体控制要求	华为云的内部实践	客户的职责
4.1.1	<p>定义[密码学要求]，考虑以下因素：</p> <ul style="list-style-type: none"> • 定义基本加密协议和技术（例如 AES 256、RSA 2048 和 PKI）以及相关限制（例如自签名证书、MD-5） • 应应用经批准的加密协议的条件（传输中的、静止的、使用中的数据）以及所需的保护级别 	华为云制定并实施密码算法应用规范，规定了密码算法的选择规则及应用规则，同时给出了常见应用实例指导。华为云自身使用行业广泛使用的 AES 强效加密法对平台内的数据进行加密，在传输过程中使用高版本 TLS 加密协议保障数据安全，确保不同状态下的数据的机密性。使用数字签名和时间戳等控制机制，防止数据传输过程中被篡改，确保信息完整性并防止重放攻击。	客户应建立密码管理政策，确保正确有效地使用密码学来保护信息资产，确保适当和有效地使用密码技术以保护信息的保密性、真实性和完整性。
4.1.2	根据相关限制（例如法律、技术、国家）创建[加密解决方案]（例如产品、算法和协议）列表，并确保其得到负责角色的批准。	华为云实施由华为云网络安全能力中心维护的密码算法应用规范，其中包含常见密码算法及方案的标准化信息列表，此列表已参考业界广泛采用标准和最佳实践，指导产品正确选择和使用密码算法。	客户在使用加密措施保护数据时，应考虑采用业内认可的加密算法和密钥管理机制。

4.1.3	根据识别的情况使用[加密解决方案]，以便根据信息的分类[信息保护要求]，在信息的整个生命周期（传输中、静止中、使用中）内保护信息。	<p>华为云建立了保护技术设备上的数据的加密策略与密钥管理机制，对人员的权限与职责分配、加密级别、加密方法进行了规定。华为云自身使用行业广泛使用的 AES 强效加密法对平台内的数据进行加密，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，传输中数据的保护通过如下方式提供：</p> <p>1. 虚拟专用网络（VPN）：用于在远端网络和 VPC 之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云。目前，华为云采用硬件实现的 IKE（密钥交换协议）和 IPsecVPN 结合的方法对数据传输通道进行加密。</p> <p>2. 应用层 TLS 与证书管理：华为云服务提供 REST 和 Highway 方式进行数据传输。</p> <p>以上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。此外，华为云提供的基础设施存储、数据库本身具有数据备份的机制，备份的数据副本和数据采用同样的数据安全措施。例如云硬盘提供安全的加密算法（AES-256）和功能、对象存储服务可提供服务端加密功能及防盗链功能、RDS 数据库提供存储加密机制等。通过与数据加密服务集成，备份数据可以方便、快速地实现加密存储，有效保证备份数据的安全性。</p>	<p>客户应定义密码的使用策略，依据数据和信息的分类级别，考虑对传输中和静态数据的加密算法的类型、强度和质量。</p> <p>客户可通过华为云的数据加密服务 DEW 实现对数据的加密，华为云将复杂的数据加解密、密钥管理逻辑进行封装，使得客户的数据加密操作变得简单易行。</p> <p>目前，华为云云硬盘（EVS）、对象存储服务（OBS）、镜像服务（IMS）和关系型数据库等多个服务均提供数据加密（服务端加密）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。</p> <p>对于传输中的数据，当客户通过互联网提供 Web 网站业务时，可以使用华为云联合全球知名证书服务商提供的证书管理服务。通过给 Web 网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输。</p>
4.1.4	定义并实施{加密密钥生命周期管	华为云制定并实施密钥管理安全规范，对密钥生命周期各阶段的安全	客户应建立密钥管理机制，用于

	理}流程, 用于处理加密密钥的生成、保护、归档、恢复和销毁。	进行管理, 明确在密钥生成、传输、使用、存储、更新、备份与恢复、销毁等阶段的安全管理要求。	处理加密密钥的生成、保护、归档、恢复和销毁, 使数据的机密性和完整性不会受到损害。 华为云为客户提供了数据加密服务(DEW), 其密钥管理功能可对密钥进行全生命周期集中管理。在未授权的情况下, 除客户外的任何人无法获取密钥对数据进行解密, 助力客户云上数据的安全。DEW 采用分层密钥管理机制, 方便各层密钥的轮换。华为云使用的硬件安全模块(HSM)为客户创建和管理密钥, HSM 拥有 FIPS140-2(2 级和 3 级) 的主流国际安全认证, 助力用户的数据合规性要求, 能够做到防入侵、防篡改, 即使是华为运维人员也无法窃取客户根密钥。DEW 还支持客户导入自有密钥作为客户主密钥进行统一管理, 方便与客户已有业务的无缝集成、对接。同时, 华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机
--	--------------------------------	---	---

			制，保障了密钥的持久性。
4.1.5	持续审查和优化[密码学要求]和批准的加密解决方案列表，以及实施的加密解决方案的有效性。	华为云每年会对建立的密码算法应用及密钥管理安全相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对密码学的网络安全要求以及流程的有效性进行审查和更新。

7.4.2 变更管理

管理对信息资产的更改，以防止未经授权和意外的修改。

编号	具体控制要求	华为云的内部实践	客户的职责
4.2.1	定义[变更管理要求]，考虑以下因素： • 对影响网络安全的信息资产的变更进行识别、分类和优先排序	华为云制定了变更管理的管理规定和变更流程，对不同变更类型应遵循的不同的变更管理流程，包括申请、评审及实施相变更进行了定义，各项变更均需通过多个环节的审核，并依据变更的紧急程度等因素对变更进行分类。	客户应建立变更管理程序，根据信息资产的重要性，对变更进行识别、分类和优先级排序。
4.2.2	定义和实施{变更管理}流程以授权网络安全相关变更（例如，应用补丁、配置变更作为补救、升级或引入新设备的一部分）。	生产环境的各要素，如网络、系统平台软硬件和应用等的更改，包括架构调整、系统软件更新、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。华为云遵循变更管理的管理规定和变更流程，各项变更均需通过多个环节的审核，需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保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，变更委员会审批通过后才可以上线。	客户应实施变更流程，对实施的变更进行授权的变更管理。
4.2.3	计划和测试已识别的更改。评估变更对网络安全的潜在影响[网络安全风险评估]，传达变更，并获得已定义的授权角色（人员/委员会）的批准。	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，都需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保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。	客户应测试已识别的变更，评估其网络安全风险，并在获得授权批准后才可以变更。

4.2.4	加强和实施[变更管理要求], 考虑紧急变更的程序。	华为云也制定了规范的紧急变更管理流程。若紧急变更影响到用户，会按规定的时限提前通过公告、邮件、电话、会议等方式与用户沟通；若紧急变更不满足提前规定的通知时限，变更将升级至华为云高层领导，并在变更实施后及时对用户公告。	客户应在变更管理要求中考虑紧急变更的流程。
4.2.5	持续审查和优化[变更管理要求]以及{变更管理}流程中使用的控制。	华为云每年会对建立的变更管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对变更管理的安全要求以及流程的有效性进行审查和更新。

7.4.3 漏洞管理

识别信息资产的漏洞以确定优先级并建议补救措施。

编号	具体控制要求	华为云的内部实践	客户的职责
4.3.1	定义[漏洞管理要求], 考虑以下因素： <ul style="list-style-type: none"> • 范围、工具和技术、报告 • 扫描频率 • 修复漏洞的时间表（基于严重性） 	华为云建立了安全漏洞管理流程，设置了漏洞管理员及相关安全角色为漏洞的评估负责，并要求了定期安全关键安全补丁，降低漏洞风险，对漏洞定级、责任分配及漏洞处理要求进行规定。同时，华为云建立了专门的漏洞响应团队，及时评估并分析漏洞的原因、威胁程度及制定补救措施，评估补救方案的可行性和有效性。	客户应建立有效的漏洞管理机制，对所有技术资产进行漏洞识别和风险评估。
4.3.2	定义并实施{漏洞管理}流程，包括： <ul style="list-style-type: none"> • 扫描：根据漏洞管理要求中定义的频率，使用相关工具对信息资产[资产清单]进行漏洞扫描（例如，关键系统每月一次） 	华为云建立了漏洞定期扫描机制，每月对报告范围内的产品执行漏洞扫描并由漏洞扫描团队负责对扫描结果进行跟踪处理。同时，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。	客户应根据漏洞扫描流程，以组织定义的频率对其信息系统进行漏洞扫描，对关键系统每月进行一次漏扫。 华为云会第一时间针对紧急爆发的通用漏洞 CVE 进行分析并更新规则，提供快

			速、专业的 CVE 漏洞扫描。
	<ul style="list-style-type: none"> 分析：分析漏洞对关键信息资产的影响，并为其分配关键性。定义并分配时间范围（取决于严重程度），在该时间范围内必须修复漏洞 	<p>华为云已建立起从漏洞感知到现网修复的端到端漏洞响应工单系统，自动根据漏洞的严重程度确定处理优先级，从而明确对应的漏洞修复 SLA 要求。对于重大安全漏洞，安全运维团队可通过自研工具，对现网进行扫描，实现分钟级的受影响服务和模块的范围界定；同时安全运维团队会根据现网情况，采取必要的漏洞缓解措施，例如限制端口访问、实施 WAF 漏洞规则等方式对受影响的服务进行防护或隔离，以降低漏洞被利用的风险。对于需要通过版本、补丁修复的漏洞，通过灰度发布或蓝绿部署等方式尽量减少对租户业务造成影响。同时，华为云还持续更新操作系统及容器镜像，通过镜像和容器的滚动升级完成系统漏洞修复，不会对租户业务造成影响。</p>	客户应根据漏洞的重要程度，定义并分配时间范围，在定义的响应时间内完成漏洞修复。
	<ul style="list-style-type: none"> 报告：向各部门报告漏洞[漏洞报告]以及资产的关键性，并确定建议的行动。[补丁管理] 	<p>华为云漏洞修复团队每月对平台侧发现的漏洞修复情况进行汇总分析，并将审阅结果记录在华为云网络安全月报中，向有关部门报告并确定整改的行动。华为云针对会影响客户服务的漏洞，华为云会发布漏洞公告，其中包括漏洞详情、漏洞原理分析、漏洞影响范围、漏洞防范措施及漏洞解决方法等内容。</p>	客户应将漏洞扫描的结果与相关部门报告，确定修复的建议方案。
4.3.3	执行由不同事件触发的漏洞扫描（例如产品发布、重大技术变更、网络中添加的新设备）。	华为云会在产品发布、重大技术变更和网络中添加新设备等场景下开展漏洞扫描活动。同时，华为云内外部的安全团队开展漏洞扫描活动需通过常规变更评审后才可进行漏洞扫描，并需要告知测试工具、目标系统、目的等，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。	客户应在产品发布、重大技术变更或网络中添加的新设备等不同场景下执行漏洞扫描。
4.3.4	使用专门的自动化漏洞扫描工具（例如用于 Web 服务器、移动应用程序的专用工	华为云的漏扫的开源和第三方工具从正规渠道获取，商业工具需具备合法授权。	客户可使用专门的自动化漏扫工具进行漏洞扫描工作。 华为云会第一时

	具)。		间针对紧急爆发的通用漏洞 CVE 进行分析并更新规则，提供快速、专业的 CVE 漏洞扫描。
4.3.5	根据其他来源(例如渗透测试、威胁情报)的输入加强漏洞分类和报告。	华为云已建立起从漏洞感知到现网修复的端到端漏洞响应工单系统，此系统会自动接收来自 PSIRT、在线扫描工具等众多漏洞收集渠道提交的漏洞，并自动根据漏洞的严重程度确定处理优先级，从而明确对应的漏洞修复 SLA 要求。通过建立包括云业务在内的所有产品和解决方案的公司级漏洞库，以保证有效记录、追踪和闭环每个漏洞。	客户应根据渗透测试、威胁情报等网络安全资源作为输入加强漏洞分类和报告。
4.3.6	持续审查和优化[漏洞管理要求]以及{漏洞管理}过程。	华为云每年会对建立的漏洞管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对漏洞管理的网络安全要求及流程的有效性进行审查和更新。

7.4.4 补丁管理

确保在适当的时间范围内将安全补丁应用于信息资产，以修复已知问题并增强其弹性。

编号	具体控制要求	华为云的内部实践	客户的职责
4.4.1	<p>定义[补丁管理要求]，考虑以下几点：</p> <ul style="list-style-type: none"> • 补丁管理范围 • 工具和技术以及补丁管理的触发 • 补丁测试环境 • 频率（包括定期修补） 	华为云建立安全补丁管理的流程，保证安全补丁在 IT 安全标准规定的期限内完成安装。同时，华为云制定了漏洞管理机制，确保对云平台及云服务安全漏洞及时的应急响应，根据漏洞整改要求，针对不同严重程度的漏洞修复时限要求及时在规定的期限内应用修补措施或补丁、补丁装载前置于研发阶段和灵活简化安全补丁部署周期等。补丁安装时有专门的工具和平台，并且在升级实施前先在测试环境或类生产环境验证，再对生产环境升级，生产环境灰度操作，分批实施。	客户应制定适用的补丁管理安全要求，确保及时将安全补丁应用于信息资产中，以修复发现的漏洞。

4.4.2	定义和实施{补丁管理}流程，制定[补救计划]，考虑以下方面： <ul style="list-style-type: none">• [漏洞报告]• [网络安全风险评估]• 在生产部署之前测试补丁并根据风险评估结果创建必要的备份• [变更管理]• 定期发布补丁	华为云针对漏洞扫描、风险评估等安全活动识别的漏洞和风险，使用专门的工具平台对不同组件进行补丁发布及升级，在云服务产品上线发布前，云服务团队需对服务发布包（包含补丁包）进行病毒扫描和完整性校验。华为云依托其建立的漏洞管理体系进行漏洞管理，使基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在 SLA 时间内完成响应和修复。对于需要通过版本、补丁修复的漏洞，通过灰度发布或蓝绿部署等方式尽量减少对用户业务造成影响。华为云会定期针对不同组件发布标准补丁版本，各云服务、云平台须在规定时间内完成适配，如 OS 补丁版本基线每年发布一次。	客户应建立有效的补丁和漏洞管理机制，对所有技术资产进行漏洞识别和风险评估，对关键补丁进行测试，制定补丁更新周期以及补丁修复的工作流程。 华为云镜像服务(IMS)简单方便的镜像自助管理功能。客户可通过服务控制台或 API 对自己的镜像进行管理。华为云负责公共镜像的定期更新与维护向用户提供安装安全补丁的公共镜像和相关安全加固和补丁信息以便用户在部署测试、故障排除等运维活动时参考。
4.4.3	确保已安装的补丁程序成功并且已修复检测到的漏洞。	华为云服务团队需根据安全漏洞验收标准确保在验收之前提供符合要求漏洞补丁。安全运维参照安全验收标准完成安全漏洞的验收。	客户应确保已安装的补丁程序成功并且已修复检测到的漏洞。
4.4.4	加强和实施[补丁管理要求]，包括针对高度关键漏洞的紧急补丁活动。	华为云制定并实施补丁版本基线管理要求，其中明确了对于重大安全漏洞，运维团队将单独发布紧急修补版本或补丁，各云平台和云服务团队参照华为云漏洞管理规范在规定的时间范围内完成修复。	客户应确保补丁管理要求中包含针对高度关键漏洞的紧急补丁活动。
4.4.5	定期为所有信息资产应用补丁包(或软件更新)。	华为云建立了安全漏洞管理流程，设置了漏洞管理员及相关安全角色为漏洞的评估负责，并要求了定期安全关键安全补丁，降低漏洞风险。	客户应定期为所有信息资产应用补丁包。
4.4.6	尽可能自动化并实施补丁管理(例如终端用户设	华为云对不同的系统组件，均使用了专门的工具平台进行补丁发布及升级，可支持自动化的补丁部署。同时，华为云会针对不同类型的补	客户可使用自动化的补丁管理工具。

	备)。	丁进行评估，决策是哪些场景可自动部署补丁，哪些场景需要专业人员手动部署，最大限度地减少补丁对系统的安全性和可用性造成负面影响。	
4.4.7	加强[补救计划]并根据威胁情报、[渗透测试]等来源执行。	华为云已建立起从漏洞感知到现网修复的端到端漏洞响应工单系统，此系统会自动接收来自 PSIRT、在线扫描工具等众多漏洞收集渠道提交的漏洞，并自动根据漏洞的严重程度确定处理优先级，从而明确对应的漏洞修复 SLA 要求。通过建立包括云业务在内的所有产品和解决方案的公司级漏洞库，以保证有效记录、追踪和闭环每个漏洞。	客户应根据渗透测试、威胁情报等网络安全资源作为输入制定漏洞补救计划。
4.4.8	持续审查和优化[补丁管理要求]和{补丁管理}流程。	华为云每年会对建立的补丁管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对补丁管理的网络安全要求及流程的有效性进行审查和更新。

7.4.5 网络安全

保护组织运营的网络免受恶意活动的侵害，并确保网络能够抵御网络威胁。

编号	具体控制要求	华为云的内部实践	客户的职责
4.5.1	定义[网络安全要求]，考虑以下因素： <ul style="list-style-type: none">• 管理和控制组织运营的网络和与其连接的信息资产的安全性• 网络隔离• 保护网络服务和通过网络传输的信息的安全要求	华为云遵循华为公司建立的网络安全管理规定，其中明确了网络隔离、网络接入安全、网络安全防御等相关控制要求，确保组织免受网络恶意入侵造成网络安全风险。华为云实施正式的环境隔离机制，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次安全隔离。同时华为云构建了多层次防护措施，如使用接入控制和边界防护技术以实现对外来攻击的统筹防护，严格执行相应的管控措施，确保华为云安全。	客户应建立正式的系统以及网络管理程序，确保组织的网络免受安全风险。
4.5.2	记录清楚反映网络实际状态的[网络计划]（例如，	华为云会维护最新的网络拓扑结构图。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	客户应记录网络实际状态的网络

	网络的所有连接、网络设备、关键服务器）。	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。	拓扑结构。
4.5.3	确保根据[网络安全要求]对传入和传出流量进行控制（例如防止恶意流量、监控交换设施的流量负载、控制不需要的通信，如电子邮件、SMS）。	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。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。	客户应确保对传入和传出流量进行控制。 客户可通过 Anti-DDoS 流量清洗服务实现对网络层和应用层的 DDoS 攻击防护，Anti-DDoS 为客户提供精细化的防护服务，客户可以根据业务的应用类型，配置流量阈值参数，并通过实时告警功能查看攻击和防御状态。
4.5.4	确保只允许受信任和授权的协议和 IP 地址范围跨越边界（例如防火墙）。在设备上禁用未使用的协议（例如 IPv6）以减少网络上的攻击面。	华为云通过配置防火墙策略限制对高危端口及高危协议的使用。同时华为云内部制定了产品通信矩阵，其中对可使用的通信端口进行了维护，端口必须限定确定的合理的范围，且未在矩阵中的端口必须关闭，并通过端口扫描工具验证。	客户应制定安全管理策略限制对端口及协议的使用。
4.5.5	保护通过组织网络传输的信息（如防止截获、复制、修改），并确保信息的机密性和完整性得到维护（如加密）。	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，传输中数据的保护通过如下方式提供： 1. 虚拟专用网络（VPN）：用于在远端网络和 VPC 之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云。目前，华为云采用硬件实现的 IKE（密钥交换协议）和 IPsecVPN 结合的方法对数据传输通道进行加密。 2. 应用层 TLS 与证书管理：华为云服务提供 REST 和 Highway 方式进行数据传输。 以上数据传输方式均支持使用传输	客户应制定安全措施保护通过组织网络传输的信息。 客户可使用华为云提供的虚拟专用网络（VPN）、云专线服务、云连接等服务，实现不同区域之间业务的互联互通和数据传输安全。目前 VPN 服务采用华为公司专业设

		<p>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。</p>	<p>备，基于 IKE 和 IPsec 协议在 Internet 网络上虚拟出私有网络，在本地数据中心和华为云 VPC 之间、华为云不同区域的 VPC 之间构建安全可靠的加密传输通道。</p> <p>云专线服务 (DC) 基于运营商多种类型的专线网络，在本地数据中心与华为云 VPC 之间构建专享的加密传输通道，各客户专线之间物理隔离，满足更高的安全性、稳定性要求。此外，对于传输中的数据，当客户通过互联网提供 Web 网站业务时，可以使用华为云联合全球知名证书服务商提供的证书管理服务。通过给 Web 网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输。</p>
4.5.6	根据这些区域中存在的信息资产或服务的重要性（例如，将生产网络与开发和测试网络隔离，将包含用户工作站的网络与身份验证服务器分开），将网络划分为多个区域（例如域、子网）。	<p>华为云参考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。</p> <p>华为云数据中心主要分为以下五个</p>	客户应根据网络区域中存在信息资产或服务的重要性，将网络划分为多个区域。

		<p>重要安全区域：DMZ 区、公共服务区（Public Service）、资源交付区（POD – Point of Delivery）、数据存储区（OBS – Object -Based Storage）、运维管理区（OM – Operations Management）。除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能，确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的 OM 区，攻击面最小，安全风险相对容易控制。</p> <p>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，提升面对外部入侵和内部违规操作的自我保护和容错恢复能力，降低对运行环境未授权访问或变更的风险。</p> <p>华为云对云端数据的隔离是通过虚拟私有云（VPC – Virtual Private Cloud）实施的，VPC 采用网络隔离技术，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置：一方面，结合 VPN 或云专线，将 VPC 与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用 VPC 的 ACL、安全组功能，按需配置安全与访问规则，满足租户更细粒度的网络隔离需要。</p>	
4.5.7	根据访问控制列表[身份和访问管理和特权访问管理]限制对组织网络（有线和无线网络）的访问。	华为云所有接入华为内部网络包括有线办公网络和无线办公网络的计算机设备均必须安装公司安全软件，员工可通过公司安全软件从外部网络接入华为内部办公网络。此外，未经批准，在华为办公区域内，不允许接入非华为提供的无线网络，禁止在华为办公区域私自搭建无线网络或将测试无线网络接入公司办公网络，若有业务需求，必须经过业务主管和 IT 管理部门评估和审核批准。此外，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	客户应制定访问控制策略限制对组织网络的访问。

		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。	
4.5.1 1	加强并实施[网络安全要求]，以应对针对组织网络的内部和外部攻击（如 DoS/DDoS）。	华为云在网络边界部署 DoS/DDoS 防范清洗层、下一代防火墙、入侵防御系统层以及网站应用防火墙层，在内部根据业务功能和网络安全风险将数据中心划分为多个安全区域，实现物理和逻辑控制并使用隔离手段，提升网络面对入侵和内鬼的分区自我保护和容错恢复能力。	客户可部署入侵防御系统，以应对针对组织网络的内部和外部攻击。
4.5.1 2	确保在 ICT 设施中建立机制来检测和避免导致服务中断的网络拥塞（例如，实施额外的设施来平衡流量负载）。	华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可以充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。	客户应确保在 ICT 设施中建立机制来检测和避免导致服务中断的网络拥塞。 客户可通过华为云弹性负载均衡（ELB - Elastic Load Balance）将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。
4.5.1 3	使用特定工具分析和过滤所有流量（例如端口过滤、基于主机的过滤），以检测网络中任何未经授权的流量。	华为云使用负载均衡、DNS 和 Web 应用防火墙过滤外部流量，以监测网络中任何未经授权的流量，未经授权的或恶意流量将被拦截。	客户应使用特定工具分析和过滤所有流量，以检测网络中任何未经授权的流量。 客户可使用华为云云解析服务（DNS - Domain Name Service），华为云 DNS 提供高可用、高扩展的权威 DNS 服务和 DNS 管理服务，同时提供 Anti-DDoS 功能，对访问流量进行特征模拟，

			清洗攻击流量，限流和屏蔽恶意 IP 访问，保障服务安全稳定运行。DNS 提供的七层防护算法，逐层对攻击流量进行清洗过滤，实现了对流量层攻击和应用层攻击的全面防护。此外，客户可通过部署 Web 应用防火墙（WAF - Web Application Firewall）对网站业务流量进行多维度检测和防护。Web 应用防火墙可结合深度机器学习智能识别恶意请求特征和防御未知威胁，通过对 HTTP(S) 请求进行检测，识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，全面避免网站被黑客恶意攻击和入侵，保护 Web 服务安全稳定。
4.5.1 4	持续审查和优化 [网络安全要求] 以及组织电信网络安全所需的控制措施。	华为云每年会对建立的网络管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对网络安全的安全要求进行审查和更新。

7.4.6 日志与监控

监控和保护信息资产的事件日志，并报告任何需要进一步调查的可疑活动。

编号	具体控制要求	华为云的内部实践	客户的职责
4.6.1	<p>定义[日志和监控要求]，考虑以下因素：</p> <ul style="list-style-type: none">•记录与组织的信息资产相关的事件日志（需要监控）•监控事件日志并分析检测到的事件•事件日志所需的保留期和保护	华为云建立了安全日志管理规范，规范了华为云应用系统、服务、网络设备安全日志的管理。同时，华为云建立了集中、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，以确保支撑网络安全事件回溯，日志会保留合理的期限并实施保护措施避免未经授权的篡改、泄露等安全风险。	客户应制定事件日志与监控的安全管理策略，及时发现系统中可能存在的网络入侵的安全风险。
4.6.2	开启事件日志并记录与信息资产相关的事件日志（例如用户活动、异常、信息安全事件、特权操作）。	华为云建立了统一的日志分析平台，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。	<p>客户应收集所有关键信息资产上的网络安全事件日志。</p> <p>华为云提供的云日志服务（LTS - Log Tank Service）提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。</p>
4.6.3	保护日志信息和日志记录设施，防止未经授权的访问和篡改。	在日志保存过程中采取安全措施防止日志被篡改，以确保支撑网络安全事件回溯和合规。为确保日志数据安全，安全日志会进行统一备份或归档，并依照数据安全管理的要求，限制安全日志使用的申请及权限，仅允许授权人员因必要原因进行安全日志的查询，确保受控使用。华为云遵从法律法规要求，具备集中、完整的日志审计系统，具备强大的数据保存及查询能力，确	客户应保护日志信息和日志记录设施，防止未经授权的访问和修改。

		保所有日志内容保存时间超过 6 个月。内部人员运维操作均被日志平台采集并记录。	
4.6.4	定期审查事件日志，并向责任人员报告可疑事件和检测到的异常情况[事件管理]。	对于集中存储安全日志的日志分析平台，系统管理员会定期例行对采集状态、存储状态进行检查，保证安全日志的可用性。华为云日志分析平台对产品相关运维系统、服务器及网络设备的安全日志进行了收录，同时在平台内预设了异常操作规则，用于识别用户进行异常操作的情形，自动生成告警信息并推送至相关安全部门进行后续跟进处理。异常告警按照服务等级协议要求及时处理并通过事件分析处理平台进行实时大屏监控与记录。	客户应定期审查事件日志，并向责任人员报告可疑事件和检测到的异常情况，及时检测安全和事件。 华为云提供的云日志服务（Log Tank Service，简称 LTS）提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。结合云监控服务（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。客户可以对用户登录日志进行实时监控，当遇到恶意登陆行为可触发告警并拒绝该 IP 地址的请求。
4.6.5	将日志保留在要求中规定时间内（例如 12 个月）。	日志分析系统有强大的数据保存及查询能力，确保所有日志保存时间为 12 个月。	客户应确保网络安全事件日志的保留其必须为 12 个月。 华为云的云审计服务（Cloud Trace Service，简称 CTS）可以实时、系统地记录用户通过云账户登录管理控制台

			执行的操作。客户可根据企业对日志保留期限的要求购买不同规格的对象存储服务服务（Object Storage Service，简称 OBS）以实现日志的备份。
4.6.6	使用包含高级检测和集成功能的日志管理工具（如 SIEM）收集、监控和分析事件。	华为云建立了集中、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，以确保支撑网络安全事件回溯。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM - Security Information and Event Management）系统如 ArcSight、Splunk 对接。	客户应使用必要的技术对网络安全事件日志进行收集和分析。
4.6.7	实时监控和审查关键信息资产的事件日志。	华为云日志分析平台对产品相关运维系统、服务器及网络设备的安全日志进行了收录，同时在平台内预设了异常操作规则，用于识别用户进行异常操作的情形，自动生成告警信息并推送至相关安全部门进行后续跟进处理。异常告警按照服务等级协议要求及时处理并通过事件分析处理平台进行实时大屏监控与记录。	客户应建立监控平台对各个系统的安全日志进行持续监控和必要分析，及时检测和响应安全事态和事件。 华为云提供的云日志服务（Log Tank Service，简称 LTS）提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。结合云监控服务（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。

			客户可以对用户登录日志进行实时监控，当遇到恶意登陆行为可触发告警并拒绝该 IP 地址的请求。
4.6.8	通过使用专用工具（如安全情报工具）改进事件检测方法。更新日志管理工具的规则。	华为云具备多渠道多类型的权情报来源，并使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。支持众多威胁分析模型和算法，结合威胁情报和安全咨询，精准识别攻击。并且该系统实时评估华为云安全状态，分析潜在风险，并结合威胁情报进行预警，做好预防工作。	客户应使用专用工具（如安全情报工具）改进事件检测方法，持续收集、监控和分析安全事件。态势感知（SA - Situation Awareness）是华为云为客户提供的安全管理与态势分析平台。能够检测出包括 DDoS 攻击、暴力破解、Web 攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等多种云上安全风险。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为客户呈现出全局安全攻击态势，帮助客户识别、收集及获取信息安全事件相关证据并通过分析事件以减少事件在未来发生的可能性和影响。同时态势感知可以关联 DDoS 高防、企业主机安全服务、Web 应用防火墙和数据库安全服

			务等，集中呈现安全防护状态。
4.6.9	持续审查和优化[日志和监控要求]以及日志和监控的有效性。	华为云每年会对建立的安全日志管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对事件日志与监控管理的网络安全要求以及流程的有效性进行审查和更新。

7.4.7 身份和访问管理和特权访问管理

管理访问权限并实施适当的身份验证机制，以防止对信息资产的未经授权的访问。

编号	具体控制要求	华为云的内部实践	客户的职责
4.7.1	定义[身份和访问管理要求]，考虑以下因素： <ul style="list-style-type: none">• 用户帐户、特权帐户、授予和撤销访问权限• 认证和授权要求（例如，在远程访问的情况下，双因素身份验证）• 定义密码管理	华为云制定了公司用户账号权限管理的要求，规范华为云员工在申请、维护和注销权限时应遵循的流程。同时，华为云制定了运维账号的生命周期管理，包括帐号的开销户管理、帐号责任人/使用人管理、口令管理、开销户监控管理等，帐号一旦建立，立即纳入帐号管理员的日常维护管理工作。所有运维帐号，所有设备及应用的帐号均实现统一管理，并通过统一审计平台集中监控，并且进行自动审计。以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。此外，针对华为云云平台账号，华为云制定了公有云账号权限管理要求及流程，明确了对账号的分类管理和访问控制策略。对云服务的访问通过统一身份认证服务（IAM - Identity and Access Management）对用户进行访问控制和权限管理。同时，华为云制定了密码策略及账号口令安全相关管理规范。	客户应建立身份认证与访问控制管理机制，对访问系统的行为进行权限限制和监督。 客户可通过华为云的统一身份认证服务（Identity and Access Management，简称 IAM）对使用云资源的用户账号进行管理。华为云统一身份认证服务提供适合企业级组织结构的用户账号管理服务，为客户分配不同的资源及操作权限。
4.7.2	定义并实施{分配/撤销用户权限}的流程，考虑：		
	根据用户被授权使用的内容（例如基于角色的访问控制）向用户分配访问权限	华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访	客户应实施基于角色的访问控制及权限管理，符合按需知晓和使用的最小原则。

		问。	客户可使用华为云统一身份认证服务，可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。
	<ul style="list-style-type: none">在工作职能发生变更时（如更换部门）重新分配用户访问权限；合同协议变更时（如终止雇佣关系、部门变更），撤销对信息系统的访问权限。	华为云已规定对不同级别账号/权限的最长审视周期，账号/权限责任人会定期审视其持有的账号/权限，在使用人转岗或角色变化时由责任人提交注销申请。针对外包合作人员账号/权限，管理负责人在外包合作人员离场或不再需要账号/权限时提交注销申请。主管会审视下属的账号/权限持有情况是否合理，如下属岗位/角色变动，将审视其原有岗位账号/权限是否已注销。	客户应定期审视账号权限范围，确保用户权限申请、变更或回收时，均可以按照身份和访问控制策略进行及时的管理。
	根据访问控制原则（例如，需要知道、需要使用、最小权限原则和职责分离）管理用户身份验证和授权，并维护最新的[访问控制列表]	华为云员工在内部办公网络中使用唯一身份标识，已建立完善的账号生命周期管理规定及流程。对云服务的访问通过统一身份认证服务（IAM - Identity and Access Management）对用户进行访问控制和权限管理。所有运维账号，设备及应用的账号均进行统一管理，以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。如果账号使用人要使用账号，账号管理员可启动授权流程，通过口令或者提升账号的权限等方式进行授权；账号的申请人和审批人不能是同一个人。此外，华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访问。	客户应实施基于角色的访问控制及权限管理，符合按需知晓和使用的最小原则。客户可使用华为云统一身份认证服务，可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。

4.7.3	控制和限制特权访问权限的分配和使用。	<p>华为云针对特权账号制定了管理要求，将特权账号分类并在特权账号创建、回收、授权、使用、注销等各阶段中遵守管理要求。华为云强调员工云服务账号的安全风险可控，严格要求安全强口令，定期审视账号权限范围，特权账号被严格纳管回收。</p> <p>特权账号管理系统将日常或应急运维的功能账号或技术账号绑定到运维团队或个人。仅在员工职责所需时，对其授予特权或应急账号。所有特权或应急账号的申请需要经过多级的评审和批准。华为云仅会在得到客户授权后登录租户的控制台或者资源实例协助客户进行维护。堡垒机上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人。</p>	<p>客户应建立特权账号的管理机制，密切监督特权账号的使用。</p> <p>客户可通过华为云统一身份认证服务可以更有效地细化管理特权账户。客户也可通过云审计服务(Cloud Trace Service，简称CTS)作为辅助，CTS为客户提供云服务资源的操作记录，供用户查询、审计和回溯使用。</p>
4.7.4	为访问敏感和关键信息系统以及远程访问提供多因素身份验证。	<p>华为云使用 IAM 对访问进行管理，支持多因素认证用于登录验证和操作保护，员工每次登陆均需要使用多重身份验证确定身份。员工通过互联网访问华为云办公网时须通过支持注册认证的设备及账号密码双因素认证的虚拟专属网络(VPN)方可登录认证。此外，运维人员接入华为云管理网络对系统进行集中管理时，需使用员工身份账号，且要求使用双因子认证，如 USB key、Smart Card 等。员工账号用于登录 VPN、堡垒机，实现用户登录的深度审计。</p>	<p>客户应对远程访问进行多因素身份验证策略。</p> <p>客户可使用华为云统一身份认证服务，在密码认证通过后，还将收到一次性短信验证码进行二次认证。修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。</p>
4.7.5	实施已定义的密码管理(例如，使用强密码进行身份验证，定期更改密码)，并确保用户身份验证信息不会被泄露(例如，在身份验证信息传输期间使用加密机制)。	<p>华为云制定了密码策略及账号口令安全相关管理规范，包括规定密码长度、复杂度、更改周期，密码中不允许包含用户 ID，不可使用易被破解的常用口令以及最近 5 次使用过的密码等。对秘密鉴别信息的分配进行管理。新建系统中的账号密码在首次使用前由用户进行更改，当用户需要重置密码时对其进行验证。</p>	<p>客户应定义并实施密码策略，规范强密码策略，确保用户身份验证信息不会被泄露。</p> <p>华为云统一身份认证服务支持基于用户组的权限管理机制，支持设定符合客户条件的密码策略、</p>

			密码更改周期等策略。
4.7.6	在特定次数的登录失败尝试（例如 5 次登录尝试）后锁定帐户，并在重新授权访问之前调查重复的帐户锁定 [日志和监控]。	华为云设置了不成功的登录尝试阈值以预防无限制的非法密码登录尝试，目前最大的密码登录尝试次数是 5 次。对于系统、中间件和网络基础设施的成功和失败的登录尝试均保留日志记录，通过定期的日志审查和日志告警，对非法登录或非法登陆未遂事件进行报告。	客户应设定特定次数的登录失败尝试，在登录失败后对账户进行锁定和调查。 华为云统一身份认证服务支持基于用户组的权限管理机制，支持设定符合客户条件的登录策略、账号锁定策略、账号停用策略及会话超时策略，提供基于 IP 的 ACL。
4.7.7	定期审查用户身份和访问权限（审查频率应考虑到不同的帐户类型、信息资产的重要性等），并确保符合访问控制原则（例如，资产所有者应定期审查用户访问权限）。	华为云已规定对不同级别账号/权限的最长审视周期，账号/权限责任人会定期审视其持有的账号/权限，在使用人转岗或角色变化时由责任人提交注销申请。针对外包合作人员账号/权限，管理负责人在外包合作人员离场或不再需要账号/权限时提交注销申请。主管会审视下属的账号/权限持有情况是否合理，如下属岗位/角色变动，将审视其原有岗位账号/权限是否已注销。	客户应定期审视账号权限范围，确保用户权限申请、变更或回收时，均可以按照身份和访问控制策略进行及时的管理。
4.7.8	加强和实施[身份和访问管理要求]，使用工具实现身份和访问管理的自动化和集中化。	华为云员工在内部办公网络中使用唯一身份标识，已建立完善的账号生命周期管理规定及流程。对云服务的访问通过统一身份认证服务（IAM - Identity and Access Management）对用户进行访问控制和权限管理。所有运维账号，设备及应用的账号均进行统一管理，以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。此外，华为云所有运维账号实现统一管理，以确保实现从创建用户、授权、鉴权到权限回收的全流程管理，并通过统一审计平台集中监控，并且进行自动审计。	客户应使用工具实现身份和访问管理的自动化和集中化。 客户可通过华为云的统一身份认证服务对使用云资源的用户账号进行管理。华为云统一身份认证服务提供适合企业级组织结构的用户账号管理服务，为客户分配不同的资源及操作权限。

4.7.9	对需要管理访问权限的任务使用专用系统。	华为云基于堡垒机账号认证授权审计，杜绝了身份管理风险。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。确保运维人员在目标主机上的操作行为都可以定位到个人。特权账号管理系统将日常或应急运维的功能账号或技术账号绑定到运维团队或个人。	<p>客户应对需要管理访问权限的任务使用专用系统。</p> <p>客户可通过华为云云堡垒机（CBH - Cloud Bastion Host）实现集中的帐号、授权、认证和审计管理。CBH 可以灵活部署在客户网络中，为客户提供账号管理、身份认证、自动改密、资源授权、实时阻断、同步监控、审计回放等能力，增强运维管理的安全性，具备强大的输入输出审计能力。</p>
4.7.10	持续审查并优化 [身份和访问管理要求]。	华为云每年会对建立的身份与访问管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对身份与访问管理的网络安全要求进行审查和更新。

7.4.8 应用程序白名单

创建并执行在组织内授权安装和使用的软件应用程序列表。

编号	具体控制要求	华为云的内部实践	客户的职责
4.8.1	<p>定义[应用白名单的要求]，考虑以下事项：</p> <ul style="list-style-type: none"> • 授权软件列表 • 批准的应用程序白名单工具 	华为云制定并实施桌面终端服务软件标准及开源软件清单，仅可以使用户其中定义的标准操作系统和软件应用程序。此外，华为云制定了安全编程规范及应用安全开发规范，其中明确了华为云可使用的软件库和数字签名脚本，避免恶意软件的入侵造成安全风险。在终端设备上	客户应建立应用程序白名单的要求，并可使用应用程序白名单管理工具保护组织信息资产上仅执行授权软件。

		的 iDesk 程序设有上审阅后的应用程序白名单，华为云内部办公软件仅能从该平台进行下载。	
4.8.2	建立并发布[授权软件索引]，包括软件应用程序、软件库（例如 *.dll、*.ocx、*.so）和数字签名脚本（例如 *.ps1、*.py、macros）。	华为云制定并实施桌面终端服务软件标准及开源软件清单，仅可以使用户其中定义的标准操作系统和软件应用程序。此外，华为云制定了安全编程规范及应用安全开发规范，其中明确了华为云可使用的软件库和数字签名脚本，避免恶意软件的入侵造成安全风险。	客户应基于白名单技术，明确组织内授权安装和使用的软件、软件库和数字签名脚本。
4.8.3	定期审查和更新 [授权软件索引]。	华为云安全团队定期对软件白名单进行审查和更新，确保白名单的持续有效性，以防止信息资产被恶意软件入侵。	客户应定期对指定的白名单进行审查和更新。
4.8.4	使用应用程序白名单工具确保所有信息资产上仅执行授权软件，并确保不能禁用或绕过应用程序白名单技术。	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。针对使用桌面云管理程序的华为云设备，通过在后台系统进行配置的方式确保员工无法自行卸载或禁用。	客户应确保组织信息资产上仅执行授权软件，并确保不能禁用或绕过应用程序白名单技术。
4.8.5	持续审查和优化 [应用程序白名单要求]以及应用程序白名单的有效性。	华为云每年会对建立的应用程序白名单相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对应用程序白名单管理的网络安全要求及流程的有效性进行审查和更新。

7.4.9 事件管理

检测和响应网络安全事件，以遏制和最大限度地减少事件的影响。

编号	具体控制要求	华为云的内部实践	客户的职责
4.9.1	定义[事件管理要求]，考虑以下因素： • 事件定义、识别和分类、优先级和响应	华为云内部制定了安全事件管理机制，规范了华为云安全事件响应操作，明确华为云安全事件定级及通报机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云每年对信息安全事件管理程序和流程进行	客户应制定网络安全事件管理策略，建立安全事件上报和决策流程，并采取适当应对计划和沟通策略。

	<ul style="list-style-type: none">• 事件报告结构• 测试事件响应流程• 证据收集• 从信息安全事件中学习	测试，所有的安全事件响应人员，包括后备人员均需参与。	
4.9.2	定义并实施{事件响应}流程，考虑： 通过分析报告的事件进行事件检测[日志和监控]。 基于要求中规定的预定义标准的事件分类。 在组织规定的时间范围内响应信息安全事件（控制、消除和恢复）[变更管理]。 准备[事件报告]和经验教训。		
	通过分析报告的事件进行事件检测[日志和监控]。	华为云日志分析平台对产品相关运维系统、服务器及网络设备的安全日志进行了收录，同时在平台内预设了异常操作规则，用于识别用户进行异常操作的情形，自动生成告警信息并推送至相关安全部门进行后续跟进处理。异常告警按照服务等级协议要求及时处理并通过事件分析处理平台进行实时大屏监控与记录，华为云安全事件响应团队负责监控和分析告警，评估是否属于信息安全事件，并针对收集上来的安全事件进行统一的跟踪管理，确保安全事件得以被及时处理及修复。	客户应遵循已制定的网络安全事件管理策略，对各个系统的安全日志进行持续监控和必要分析，及时检测和响应安全事态和事件。
	基于要求中规定的预定义标准的事件分类。	华为云内部制定了完善的事件管理流程，根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的处理时限。在事件发生后，华为云将根据事件的优先级，在规定的时限内对事件进行响应和解决，最大化降低事件对客户造成的影响。	客户应根据事件的影响程度和范围的不同对网络安全事件进行分类。
	在组织规定的时间范围内响应信息安全事件（控制、消除和恢复）[变更管理]。	在出现安全事件时华为云依照事件响应流程（识别、评估、决策和执行应急响应处理），根据不同类型及级别的安全事件实施响应机制，在事件发生后，华为云将根据事件的优先级，在规定的时限内对事件进行响应和解决，最大化降低事件对客户造成的影响。	客户应制定安全事件响应计划，明确不同安全事件的响应流程，在安全事件发生时，根据已制定的流程对安全事件进行响应。
	准备[事件报告]和经验教训。	华为云有专业的安全事件管理系统，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，对	客户应利用在分析和解决信息安全事件中得到的知识来减少未来

		安全事件进行端到端的跟踪闭环，保证整个处置过程可回溯，并形成事件报告总结经验教训，在报告中告知事件的描述、起因、影响、华为云已采取的措施等内容。此外，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。	事件发生的可能性和影响。
	向 CST 报告具有适当详细信息的重大事件。	华为云针对安全事件带来的影响及处理流程进行回顾总结，并按照要求通知、汇报至相应受影响的用户及监管部门。华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。 为配合客户满足网络安全事件上报 CST 的要求，华为云设置 7*24 的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。	当发生网络安全事件时，客户应按照本规定的要求向 CST 上报。
4.9.3	进行定期培训以测试{事件响应}流程的有效性（例如测试沟通渠道、响应时间）。	华为云每年对信息安全事件管理程序和流程进行培训和测试，所有的安全事件响应人员，包括后备人员均需参与。此外，华为云针对各产品可能涉及的不同突发场景，规范了应急响应工作流程，形成应急响应预案，定期做应急演练和测试，持续优化应急响应机制。	客户应定期进行培训以测试事件响应流程的有效性。
4.9.4	加强并实施[事件管理要求]，使用事件管理工具实现流程自动化，并与其他相关系统集成以提高效率。	华为云有专业的安全事件管理系统，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，对安全事件进行端到端的跟踪闭环，保证整个处置过程可回溯。华为云日志分析平台对产品相关运维系统、服务器及网络设备的安全日志进行了收录，异常告警按照服务等级协议要求及时处理并通过事件分析处理平台进行实时大屏监控与记	客户应使用事件管理工具实现流程自动化，并与其他相关系统集成以提高效率。

		录。此外，华为云使用了安全编排与自动化响应技术（Security Orchestration, Automation and Response，简称 SOAR），提供了各类 SIEM 系统数据接入，基于产生的安全事件或安全威胁，SOAR 可自定义流程场景、预置策略及响应手段，形成从分析、判断到响应的自动化编排能力。	
4.9.5	收集威胁情报，并在分析信息安全事件时使用。	华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。支持众多威胁分析模型和算法，结合威胁情报和安全咨询，精准识别攻击，并且该系统实时评估华为云安全状态，分析潜在风险，并结合威胁情报进行预警，做好预防工作。此外，华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM - Security Information and Event Management）系统如 ArcSight、Splunk 对接。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，持续的监控和实时分析保证对安全事件的及时发现。	客户应多渠道收集和分析网络威胁情报。 态势感知（SA - Situation Awareness）是华为云为客户提供的安全管理与态势分析平台。能够检测出包括 DDoS 攻击、暴力破解、Web 攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等多种云上安全风险。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为客户呈现出全局安全攻击态势，帮助客户识别、收集及获取信息安全事件相关证据并通过分析事件以减少事件在未来发生的可能性和影响。同时态势感知可以关联 DDoS 高防、企业主机安全服务、Web 应用防火墙和数据库安全服务等，集中呈现

			安全防护状态。
4.9.6	成立取证小组，对信息安全事件进行调查。	华为云制定了安全事件应急处置流程及响应流程，当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。	客户应成立取证小组，对信息安全事件进行调查。
4.9.7	识别、收集和保存信息安全事件的证据。利用从信息安全事件中获得的知识来降低未来事件发生的概率和影响。	华为云制定了安全事件应急处置流程及响应流程，当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。此外，华为云每年对高风险事件处理过程进行回顾，以确保高风险事件的处理过程满足公司实际的业务需求。	客户应利用在分析和解决信息安全事件中得到的知识来减少未来事件发生的可能性和影响。
4.9.8	持续审查和优化[事件管理要求]和相关的{事件响应}流程。	华为云每年会对建立的安全事件管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对事件管理的网络安全要求及流程的有效性进行审查和更新。

7.4.10 恶意软件处理

检测恶意软件并防止其在组织中传播。

编号	具体控制要求	华为云的内部实践	客户的职责
4.10.1	定义[恶意软件处理要求]，考虑以下因素： •检测和预防控制以防止恶意软件 •实施技术控制以保护组织的信息资产	华为云遵循华为公司建立的 IT 安全标准，其中明确了为防止对基础设施未经授权的变更或恶意入侵而实施的安全控制要求，包含有害代码防护、恶意软件防护等相关要求，保护组织的信息资产。	客户应定义恶意软件处理的安全要求。
4.10.2	使用终端保护软件，并确保此软件定期更新其签名数据库。采取措施防止用户停用或更改此软	在终端设备上部署了统一的终端保护软件，该软件具备保护终端设备免受恶意软件攻击的能力，且定期更新恶意软件防护机制。华为云通过在后台系统进行配置的方式确保员工无法自行卸载或禁用。	客户应使用终端保护软件，并采取措施防止用户停用或更改此软件。

	件。		
4.10. 3	实施适当的安全措施来阻止不同来源的恶意流量(例如, 使用互联网过滤器、电子邮件过滤器来阻止钓鱼邮件、限制下载危险内容)[电子邮件和基于 Web 的保护]。	华为云使用经由华为公司批准的技术手段, 如部署防病毒程序、终端准入控制等对办公网络进行安全防护。此外, 华为云部署 NDR 和防火墙过滤外部流量, 以监测网络中任何未经授权的流量, 未经授权的或恶意流量将被拦截。	客户应实施适当的安全措施来阻止不同来源的恶意流量。 客户可使用华为云云解析服务(DNS - Domain Name Service), 华为云 DNS 提供高可用、高扩展的权威 DNS 服务和 DNS 管理服务, 同时提供 Anti-DDoS 功能, 对访问流量进行特征模拟, 清洗攻击流量, 限流和屏蔽恶意 IP 访问, 保障服务安全稳定运行。此外, 客户可通过部署 Web 应用防火墙(WAF - Web Application Firewall)对网站业务流量进行多维度检测和防护。Web 应用防火墙可结合深度机器学习智能识别恶意请求特征和防御未知威胁, 通过对 HTTP(S)请求进行检测, 识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击, 全面避免网站被

			黑客恶意攻击和入侵，保护 Web 服务安全稳定。
4.10.4	实施保护措施以保护可移动介质免受恶意软件的侵害（例如，在插入或连接时对可移动介质进行反恶意软件扫描）。	华为云制定并实施移动介质管理规定，各类移动介质由专人管理，借用时需要审批，使用完毕后须进行格式化处理。对个人存储介质及数字设备进出不同安全保密级别的区域及其使用均制定了不同的安全要求，规定不得用个人存储介质连接服务器，未经授权，也不得私自使用任何存储介质连接服务器。	客户应实施保护措施以保护可移动介质免受恶意软件的侵害。
4.10.5	实施高级恶意软件检测技术（例如，启用域名系统(DNS)查询日志记录以检测已知恶意域的主机名找）。	在物理主机层面，通过部署防病毒软件，以实现对恶意软件的攻击防御。华为云桌面终端标准镜像内默认提供防病毒软件，员工默认无法对防病毒软件进行禁用操作。 此外，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。	客户应确保域名服务(DNS)的安全性。 客户可使用华为云云解析服务(DNS - Domain Name Service)，华为云 DNS 提供高可用、高扩展的权威 DNS 服务和 DNS 管理服务，同时提供 Anti-DDoS 功能，对访问流量进行特征模拟，清洗攻击流量，限流和屏蔽恶意 IP 访问，保障服务安全稳定运行。
4.10.6	使用高级日志记录和监控工具对检测到的恶意软件事件进行分析和警报[日志和监控]。	华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。华为云支持与第三方安全信息和事件管理(SIEM - Security Information and Event Management)系统如 ArcSight、Splunk 对接。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，持续的监控和实时分析保证对安全事件的	客户应使用高级日志记录和监控工具对检测到的恶意软件事件进行分析和警报。 态势感知(SA - Situation Awareness)是华为云为客户提供的安全管理与态势分析平台。能够检测出包括 DDoS 攻击、暴力

		及时发现。	破解、Web 攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等多种云上安全风险。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为客户呈现出全局安全攻击态势，帮助客户识别、收集及获取信息安全事件相关证据并通过分析事件以减少事件在未来发生的可能性和影响。同时态势感知可以关联 DDoS 高防、企业主机安全服务、Web 应用防火墙和数据库安全服务等，集中呈现安全防护状态。
4.10. 7	持续审查和优化 [恶意软件处理要求] 以及用于保护信息资产免受恶意软件传播的技术控制。	华为云每年会对建立的恶意软件防护相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对恶意软件处理的网络安全要求及技术的有效性进行审查和更新。

7.4.11 信息保护

对组织的信息进行分类，以确保对其进行充分保护。

编号	具体控制要求	华为云的内部实践	客户的职责
4.11. 1	定义[信息保护要求]，考虑以下因素： • 分类级别和标	华为云制定了数据安全策略及数据安全保护管理规定，对数据资产的分级分类标准进行了定义，同时明确了数据匿名化及标签化处理标	客户应建立正式的数据保护机制，对信息的全生命周期进行保

	<p>准（例如受限、机密、公开）{资产分类}</p> <ul style="list-style-type: none">信息的隐私、所有权、保护、传输和保留确保组织中个人信息或其 他敏感信息的隐私 [网络安全合规]	<p>准，对数据在整个生命周期中须遵循的安全措施进行了规范。同时，华为云制定了云服务安全与隐私活动操作指导，规范云服务在产品生命周期中应遵循的隐私保护要求。</p>	护
4.11. 2	<p>定义和实施{信息分类}流程，考 虑：</p> <ul style="list-style-type: none">根据要求中规 定的分类标准对 信息进行分类根据定义的标 准（例如商业价 值、法律、技 术、国家和跨境 要求）处理关键 信息	<p>华为云对数据进行分级管理，结合机密性、完整性、可用性、合规性进行综合定级，将数据分为多个安全级别并分别给出该级别数据的定义。同时规定了不同级别数据的安全实施要求、稽查要求以及应急响应及演练要求。各业务领域遵照数据定级标准对其领域内数据标记安全等级。</p>	<p>客户应依据数据 和信息的重要性 和机密性等要素 制定分类标准并 遵循规定的分类 标准对数据进行 分类和标记。</p> <p>客户可使用华为 云的数据安全中 心服务（DSC - Data Security Center）是新一代 的云原生数据安 全平台，可以为 客户提供数据分 级分类、数据安 全风险识别、数 据水印溯源、数 据脱敏等基础数 据安全能力，并 通过数据安全总 览整合数据安 全生命周期各阶 段状态，对外整体 呈现云上数据安 全态势。</p>
4.11. 3	<p>实施安全机制以 保护信息（传输 中、静止中、使 用中），同时考 虑[密码学要求] 和数据防泄漏技 术。</p>	<p>如果客户的业务数据中涉及敏感个人数据，云服务将默认加密存储该等数据，在非信任网络之间的传输的数据都是被加密的。在信息传输过程中使用安全加密信道（如 HTTPS），对存储的静态数据使用安全加密算法进行加密保护，确保不同状态下的数据的机密性。使用数字签名和时间戳等控制机制，防止数据传输过程中被篡改，确保信</p>	<p>客户应依据数据 和信息的分类级 别，考虑对传输 中和静态数据的 加密算法的类 型、强度和质 量，同时应建立 数据防泄漏机 制，并通过适当 的技术手段来防</p>

		息完整性并防止重放攻击。	止数据泄露。 客户可通过华为云的数据加密服务 DEW 实现对数据的加密，华为云将复杂的数据加解密、密钥管理逻辑进行封装，使得客户的数据加密操作变得简单易行。 目前，华为云云硬盘（EVS）、对象存储服务（OBS）、镜像服务（IMS）和关系型数据库等多个服务均提供数据加密（服务端加密）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。 对于传输中的数据，当客户通过互联网提供 Web 网站业务时，可以使用华为云联合全球知名证书服务商提供的证书管理服务。通过给 Web 网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输。
4.11.4	防止将信息从生产环境传输到另一个环境，并防止在测试和开发环境中使用关键系统数据。	华为云研发环境采取分级管理，对开发环境进行包括物理隔离、逻辑隔离、接入访问控制、数据传输通道审批及审计等保护措施。并且严格控制未脱敏的数据流入测试环境，避免生产数据或未脱敏的生产数据用于测试，使用完成后需要进行数据清理。	客户应防止将信息从生产环境传输到另一个环境，并防止在测试和开发环境中使用关键系统数据。
4.11.	根据组织要求和	华为云遵循华为公司的管理要求，	客户应确定信息

5	相关法规确定信息的保留期限，限制所需的信息保留在关键系统的生产环境中。	制定了数据留存规范，其中对各类数据的留存期限进行了规定。在存储个人数据时不超过实现数据处理目的所必要的期限。华为云定期对收集、使用、披露个人数据的目的进行审核，对不再需要的个人数据进行匿名化或删除等安全处理。	的保留期限，限制所需的信息保留在关键系统的生产环境中。
4.11.6	持续审查并优化[信息保护要求]和相关流程。	华为云每年会对建立的数据安全及隐私安全相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对信息和数据保护的网络安全要求进行审查和更新。

7.4.12 备份与恢复管理

采取必要的措施，包括备份，以确保事件发生后的信息恢复。

编号	具体控制要求	华为云的内部实践	客户的职责
4.12.1	定义[备份和恢复管理要求]，考虑以下因素的： <ul style="list-style-type: none">• 在线和离线备份的范围，包括保留期• 网络安全事件后的信息快速恢复• 定期备份信息资产• 保护备份• 备份的可用性	华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。同时，华为云制定了数据备份规范，规范华为云管理节点数据备份格式、备份时间、备份内容和策略。此外，华为云还规范了业务恢复策略的制定，确保业务能在恢复时间目标内恢复到可接受水平。	客户应制定备份与恢复的安全管理策略，定义组织对信息、软件和系统备份的要求。
4.12.2	定义并实施{备份}流程，包括在线和离线备份范围及其对信息资产的覆盖范围（例如，通过镜像等流程备份整个系统）。	华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。华为云建立了节点数据定期备份机制，通过eBackup系统实现对节点数据的备份，且备份失败时自动通过邮件发送给备份管理员进行跟进。	客户应明确关键技术和服务资产的备份范围，对关键业务数据、操作系统、应用软件进行备份。 如果客户需要对业务数据、软件和系统镜像进行备份，华为云提

			供了多种有不同侧重的产品和服务。例如，客户可以使用华为云提供的云备份（CBR - Cloud Backup and Recovery）服务对云内的云服务器、云硬盘、文件服务，云下文件、VMware 虚拟化环境进行备份，在发生病毒入侵、人为误删除、软硬件故障等导致数据不可用的场景前可将数据恢复到任意备份点。客户可使用云硬盘（EVS - Elastic Volume Service）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。华为云还为客户提供了镜像服务（IMS - Image Management Service），客户可使用该产品对云服务器的实例进行备份，当实例的软件环境出现故障时使用备份的镜像进行恢复。云服务器备份（CSBS - Cloud Server Backup Service）服务可同时为云服务器下多个云硬盘创建一致性在线备份，保护数据安全可靠，降低数据被非法篡改的
--	--	--	---

			风险。客户可以使用对象存储服务（OBS）的版本控制、云硬盘备份（VBS）、云服务器备份（CSBS）等功能，将云上的文档、硬盘、服务器进行备份。
4.12. 3	定义并实施{恢复}流程，以确保信息资产根据其重要性{资产分类}在可接受的时间范围内恢复。	华为云根据内部业务连续性管理体系的要求，为支撑云服务持续运行的关键业务制定了完善的恢复策略。恢复策略涵盖备用场地、设备、人员、信息系统、第三方等各个方面。华为云制定了业务连续性计划和灾难恢复计划，并定期对其进行测试。华为云针对各产品可能涉及的不同突发场景，规范了应急响应工作流程，形成应急响应预案，定期做应急演练和测试，持续优化应急响应机制。	客户应确保能够在发生网络安全事件后快速恢复数据和系统。 客户可使用华为云提供的镜像服务 IMS，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。
4.12. 4	实施{备份}流程，根据业务需求（例如恢复时间目标）定期对信息资产进行备份。	华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。华为云对于建立了节点数据定期备份机制，通过 eBackup 系统实现对节点数据的备份，且备份失败时自动通过邮件发送给备份管理员进行跟进。华为云支持在一个数据中心的多个节点内复制存放用户数据。单个节点一旦出现故障，用户数据不会丢失，系统可以做到自动检测和自愈。单个区域内不同可用区之间，通过高速光纤实现数据中心互联，满足跨可用区数据复制基本要求，用户可根据业务需求选择灾备复制服务。 此外，像华为云提供的存储和数据库服务均具备高可靠保证，例如 EVS 云硬盘使用多副本的数据冗余保护机制，采用副本同步写、读修复等措施保证数据一致性，当检测到硬件故障能够自动后台修复，数	客户应根据业务需求定期对信息资产进行备份。 如果客户需要对业务数据、软件和系统镜像进行备份，华为云提供了多种有不同侧重的产品和服务。例如，客户可以使用华为云提供的云备份（CBR - Cloud Backup and Recovery）服务对云内的云服务器、云硬盘、文件服务，云下文件、VMware 虚拟化环境进行备份，在发生病毒入侵、人为误删除、软硬件故障

		<p>据快速自动重建，数据持久性可达 99.9999999%。；OBS 对象存储服务通过支持对象数据的高可靠性，并通过业务节点的高可靠性网络和节点的多冗余设计，使系统设计可用性达 99.995%，完全满足对象存储服务高可用的需求，通过提供对象数据多份冗余和保证多份对象的数据一致性自动修复技术，来提供对象数据的高可靠性，系统设计数据持久性高达 99.999999999%；RDS 关系型数据库服务采用热备架构，故障系统 1 分钟自动切换。每天自动备份数据，上传到 OBS 桶，备份文件保留 732 天，支持一键式恢复。</p>	<p>等导致数据不可用的场景前可将数据恢复到任意备份点。客户可使用云硬盘（EVS - Elastic Volume Service）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。华为云还为客户提供了镜像服务（IMS - Image Management Service），客户可使用该产品对云服务器的实例进行备份，当实例的软件环境出现故障时使用备份的镜像进行恢复。云服务器备份（CSBS - Cloud Server Backup Service）服务可同时为云服务器下多个云硬盘创建一致性在线备份，保护数据安全可靠，降低数据被非法篡改的风险。客户可以使用对象存储服务（OBS）的版本控制、云硬盘备份（VBS）、云服务器备份（CSBS）等功能，将云上的文档、硬盘、服务器进行备份。</p>
4.12.5	通过物理安全[保护设备和区域]确保备份得到适当保护。	华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数	客户通过物理安全确保备份得到适当保护。

		据流转策略及访问控制策略。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。	
4.12. 6	建立备用存储/备份站点，提供与主站点相同的安全措施。	<p>客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份。所有数据中心都处于正常运营状态，无一闲置。同时，两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云要求本标准范围内的云服务均采用基于单地域多数据中心的冗余机制，以确保云服务的业务连续性。</p> <p>单个区域内不同可用区之间，通过高速光纤实现数据中心互联（DCI - Data Center Interconnect），满足跨可用区数据复制基本要求，用户可根据业务需求选择灾备复制服务。</p> <p>华为云能够在多个地域内或同一地域内多个可用区之间灵活替换计算实例和存储数据。每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。另外，各可用区有各自独立的 UPS 和现场备用发电设备，每个可用区域所连接的电网也不同，所有可用区域与多个一级传输供应商冗余相连，进一步排除单点故障的风险。此外，用户可充分利用这些地域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下（包括自然灾害和系统故障）系统都能连续运行。</p>	<p>客户应建立备用存储/备份站点，提供与主站点相同的安全措施。</p>
4.12. 7	确保在不利情况下备份的机密性、完整性和可用性（如使用加密）。	华为云提供的基础设施存储、数据库本身具有数据备份的机制，备份的数据副本和数据采用同样的数据安全措施。针对云硬盘加密算法、对象存储服务端加密、防盗链、RDS 数据存储加密机制。通过与数据加密服务集成，备份数据可以方便、快速地实现加密存储，有效保证备份数据的安全性。客户使用	<p>客户应建立监控平台对各个系统的安全日志进行持续监控和必要分析，及时检测和响应安全事态和事件。</p> <p>客户可以使用对象存储服务</p>

		VBS 云硬盘备份服务、云服务器备份服务等进行备份，加密盘的加密数据自动加密，保证数据安全。- 此外，华为云制定并实施了备份与冗余策略，包括开发测试环境、代码文档版本管理、工具软件、安全设备、生产系统的备份和冗余。华为云对于建立了节点数据定期备份机制，通过 eBackup 系统实现对节点数据的备份，且备份失败时自动通过邮件发送给备份管理员进行跟进。	(OBS) 的版本控制、云硬盘备份（VBS）、云服务器备份（CSBS）等功能，将云上的文档、硬盘、服务器进行备份。上述服务通过与数据加密服务集成，备份数据也可以方便、快速地实现加密存储，有效保证备份数据的安全性。
4.12.8	持续测试和审查{备份} 和 {恢复} 流程以检查其有效性。	华为云制定了业务连续性计划和灾难恢复计划，并定期对其进行测试。同时，华为云使用 eBackup 系统对备份数据进行循环冗余校验以确保备份数据的完整性和可用性，校验失败则无法成功进行备份。此外，华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。	客户需根据业务需求自行制定恢复测试计划，对备份的有效性进行测试。
4.12.9	加强和实施[备份和恢复管理要求]，使用工具自动化执行{备份} 和{恢复}过程。	华为云对于建立了节点数据定期备份机制，通过 eBackup 系统实现对节点数据的备份，且备份失败时自动通过邮件发送给备份管理员进行跟进。	客户应使用工具自动化执行备份和恢复流程。
4.12.10	持续审查和优化[备份和恢复管理要求]及相关流程。	华为云每年会对建立的备份与恢复和业务连续性相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对备份与恢复的网络安全要求进行审查和更新。

7.4.13 配置管理与加固

实施基线配置设置以提高信息资产的弹性。

编号	具体控制要求	华为云的内部实践	客户的职责
4.13.	定义[配置管理和	华为云对支撑业务运营的服务器操	客户应制定和实

1	加固的要求], 考虑以下内容: <ul style="list-style-type: none">信息资产和使用的软件/硬件的安全镜像和基线配置	作系统、数据库管理系统及网络设备建立了统一的基线配置标准, 以实现对服务基线配置的统一管理, 明确华为云生产环境中各系统/组件的安全配置要求, 并确保安全配置的有效执行和持续改进。华为云参考互联网安全中心 (CIS - Center of InternetSecurity) 安全基线并将融入华为云 DevSecOps 流程中并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。	施配置管理和加固的安全要求。
4.13.2	为信息资产实施定义的基线配置设置。	进入华为云生产环境的系统或组件, 由各业务交付团队按照已发布的安全配置标准进行自检, 各产品验收团队在验收时若发现不符合安全配置标准的情况, 应整改完成后才可以进入生产环境。所有产品在上线前均须由安全工程实验室按照对应的安全配置规范执行检查, 产品的配置变更均须遵从变更管理流程。	客户应为信息资产实施定义的基线配置。
4.13.3	根据行业公认的最佳实践采用系统和设备加固(例如, 禁用已安装在网络设备上的默认配置)。	华为云的运维团队根据内部的安全基线管理规范, 定期检查并更新网络设备安全参数设置。华为云对主机操作系统、虚拟机、数据库、web 应用组件等均进行安全配置加固并进行定期检查。	客户应根据行业公认的最佳实践采用系统和设备加固。
4.13.4	限制使用不必要的功能(例如使用未经授权的端口、服务)并将信息资产配置为仅提供必要的功能。	所有产品遵循华为云制定的网络安全红线中基线要求进行网络和系统的配置, 确保限制使用不必要的功能, 如禁止对 Internet 开发高危服务, 不能开放面向 Internet 的高危端口, 不能面向 Internet 的接口使用预置口令、空口令或弱口令等。	客户应限制使用不必要的功能并将信息资产配置为仅提供必要的功能。
4.13.5	根据基线设置监控和验证配置设置。	所有产品在上线前均须由安全工程实验室按照对应的安全配置规范执行检查。华为云构建了配置监控平台, 实现对服务器操作系统、数据库管理系统及网络设备的配置项进行实时监控。此外, 华为云安全运维团队按照已发布的安全配置规范和检查工具, 定期抽检华为云生产环境中各系统、组件安全配置遵从情况。	客户应根据基线设置监控和验证配置设置。
4.13.	利用专用工具监	华为云构建了配置监控平台, 实现	客户应利用专用

6	控和验证配置设置，并在未经授权偏离基线配置设置时发出告警。	对服务器操作系统、数据库管理系统及网络设备的配置项进行实时监控。配置监控平台会将实际的配置项同标准配置基线进行对比。当出现差异时，差异分析结果会通过邮件自动发送至巡检管理员进行后续跟进处理。	工具监控和验证配置设置，并在未经授权偏离基线配置设置时发出告警。
4.13.7	使用能够自动配置/重新配置所有信息资产上的配置设置[更改管理]的专用工具。	所有产品上线前都经过了多轮安全测试，其中华为云将其深入理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具，如 SecureCat 可以对业界主流的 OS 和 DB 的安全配置进行检查。此外，产品上线前均须由安全工程实验室按照对应的安全配置规范执行检查。华为云构建了配置监控平台，实现对服务器操作系统、数据库管理系统及网络设备的配置项进行实时监控。配置监控平台会将实际的配置项同标准配置基线进行对比。当出现差异时，差异分析结果会通过邮件自动发送至巡检管理员进行后续跟进处理。	客户应使用能够自动配置/重新配置所有信息资产上的配置设置的专用工具。
4.13.8	持续审查和优化[配置管理和加固要求]。	华为云每年会对建立的配置管理与加固相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对配置管理与加固的网络安全要求进行审查和更新。

7.4.14 安全软件开发

实施安全的软件开发生命周期。

编号	具体控制要求	华为云的内部实践	客户的职责
4.14.1	<p>定义[安全软件开发的要求]，考虑以下因素：</p> <ul style="list-style-type: none"> • 使用安全编码标准和实践（例如批准的库、API） • 对不同环境的访问权限的隔离 	华为云已制定开发安全管理相关制度，对华为云服务在规划、设计、开发、部署、运维和用户支撑环境应遵循的安全编程规范及应用安全开发规范进行了定义。同时，华为云规范了采用 DevOps 开发模式的产品/服务在部署和发布阶段流程，当中规范了对环境隔离的相关要求，提高生产环境稳定性。华为云及相关	客户应制定和实施安全软件开发的要求，在软件开发生命周期中实施安全策略。

	和分配 • 进行测试以验证开发的软件是否符合组织的网络安全要求	华为云服务遵从安全及隐私设计原则和规范、法律法规要求，在安全需求分析和设计阶段根据业务场景、数据流图、组网模型进行威胁分析。当识别出威胁后，设计工程师会根据削减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求、安全功能，并根据公司的测试用例库完成安全测试用例的设计，确保落地，最终保障产品、服务的安全。	
4.14.2	确保只有授权人员才能访问适当的环境[身份和访问管理和特权访问管理]。	华为云研发环境采取分级管理，对开发环境进行包括物理隔离、逻辑隔离、接入访问控制、数据传输通道审批及审计等保护措施。华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访问。	客户应确保只有授权人员才能访问其权限内的环境。
4.14.3	利用安全编码标准和实践（例如，通过静态或动态分析工具支持的安全设计原则）并确保应用程序之间的安全集成。	华为云严格遵从华为对内发布的安全编码规范。华为云服务研发和测试人员在上岗前均通过了对应规范的学习和考试。同时引入了静态代码扫描工具每日检查，其结果数据进入云服务持续集成和持续部署（CI/CD - Continuous Integration, Continuous Deployment）工具链，通过质量门限进行控制，以评估云服务产品的质量。所有云产品、云服务在发布前，均需完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。华为云使用内部 Devops 平台来实现应用安全开发生命周期中的自动构建、测试和上线部署步骤，可防止软件在环境中传输过程中被篡改。	客户应利用安全编码标准和实践确保应用程序间的安全集成。
4.14.4	确保软件在环境之间安全可靠地传输。	华为云使用内部 Devops 平台来实现应用安全开发生命周期中的自动构建、测试和上线部署步骤，可防止软件在环境中传输过程中不会被篡改。此外，华为云信息安全环境采用分区管理，禁止未经授权打通测试环境和生产环境的网络链接，避免因测试环境被入侵而导致生产环	客户应确保软件在环境之间安全可靠地传输。

		境安全风险。不允许下载源代码，不能从公司外部访问源代码，或通过基础办公应用传输源代码。源代码从公司信息安全环境传出到公司外部须审批受控。	
4.14.5	对于内部开发的软件，仅使用受信任的最新第三方组件。	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。华为云对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件退出等环节，均实施严格的管控。例如在选型分析环节，增加开源软件选型阶段的网络安全评估要求，严管选型。在使用中，须将第三方软件作为服务或解决方案的一部分开展相应活动，并重点评估开源及第三方软件和自研软件的结合点，或解决方案中使用独立的第三方软件是否引入新的安全问题。	客户应确保仅使用受信任的最新第三方组件。
4.14.6	对开发的软件和源代码进行安全审查并记录（例如，对所有输入执行错误检查）。进行安全测试，以验证开发的软件满足组织网络安全要求的程度。	华为云引入了静态代码扫描工具每日检查，其结果数据进入云服务持续集成和持续部署（CI/CD – Continuous Integration, Continuous Deployment）工具链，通过质量门限进行控制，以评估云服务产品的质量。所有云产品、云服务在发布前，均需完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。 所有云服务发布前都经过了多轮安全测试，包括但不限于 Alpha 阶段的认证、鉴权、会话安全等微服务级功能和接口安全测试，Beta 阶段通过对 API 和协议的 fuzzing 测试验证服务集成，Gamma 阶段的数据安全等安全专项测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。同时，华为云将其深入理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具，如 SecureCat 可以对业界主流的 OS 和 DB 的安全配置进行检查。	客户应进行安全测试，以验证开发的软件满足组织网络安全要求的程度。
4.14.	持续审查和优化	华为云每年会对建立的安全开发、	客户应根据计划

7	[安全软件开发要求]。	安全测试等相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	的频率定期对安全软件开发的要求进行审查和更新。
---	-------------	---	-------------------------

7.4.15 电子邮件和网络浏览器保护

保护电子邮件和 Web 浏览器免受网络安全威胁。

编号	具体控制要求	华为云的内部实践	客户的职责
4.15.1	定义 [电子邮件和 Web 浏览器保护要求] 考虑以下： <ul style="list-style-type: none">利用标准化安全机制保护电子邮件和 Web 浏览器	华为云遵循华为公司建立的办公应用系统安全，其中明确了 Email 系统、移动邮件使用、proxy 使用的安全控制要求，其中对邮件的收发规则及权限和网络浏览等进行了定义。此外，华为云遵循华为公司建立的网络安全管理规定，明确了网络接入与使用的安全规范要求，确保组织免受网络恶意入侵造成网络安全风险。	客户应制定电子邮件和 Web 浏览器保护要求。
4.15.2	实施[电子邮件和 Web 浏览器保护要求]（例如，针对垃圾邮件和钓鱼保护的电子邮件过滤、多因素身份验证、电子邮件备份和存档、针对高级持续威胁和不受信任网站的保护）。	华为云的相关人员遵循华为公司针对 Email 系统、移动邮件使用、网络接入与使用的安全控制要求。华为云使用经由华为公司批准的技术手段，如部署防病毒程序，在邮件网关对邮件进行监测和过滤，拦截病毒邮件和垃圾邮件。同时，华为云禁止在办公网络中私自启用 WWW、FTP、DNS、动态路由等网络服务或在办公网络中提供网络代理服务，同时也禁止设置所有人访问权限的共享目录。员工通过互联网访问华为云办公网时须通过支持注册认证的设备及账号密码双因素认证的虚拟专属网络（VPN）方可登录认证。此外，华为云制定了相关安全管理规定，其中明确用户在未经授权批准的情况下，禁止通过 Proxy 登录（华为 Email 之外的）私人电子邮箱，禁止通过网络向华为办公网络之外传送华为信息，禁止使用任何方式绕过 Proxy 限制向公司外传送数据或访问未授权的网站。同时也禁止设置所有人访问权	客户应实施适用的安全措施落实建立的电子邮件和网络浏览器保护要求。

		限的共享目录。同时，华为云规定所有反映华为公司工作活动且具有查考利用价值的电子邮件均属于备份和归档范围，且数据保留在在线存储介质上。	
4.15. 3	限制对未经授权的基于 Web 的电子邮件服务的访问（例如防火墙规则、基于网络的 URL 过滤器）。	华为云会限制未经授权的基于 Web 的电子邮件服务的访问，防止电子邮件地址免受欺骗、垃圾邮件和网络钓鱼之类的恶意活动的侵害。	客户应限制对未经授权的基于 Web 的电子邮件服务的访问。
4.15. 4	持续审查和优化 [电子邮件和 Web 浏览器保护要求]。	华为云每年会对建立的电子邮件、网络接入与使用管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对电子邮件和 Web 浏览器的网络安全要求进行审查和更新。

7.4.16 渗透测试

进行渗透测试以评估组织的防御能力并检测漏洞。

编号	具体控制要求	华为云的内部实践	客户的职责
4.16. 1	定义[渗透测试要求],考虑以下因素： <ul style="list-style-type: none">• 渗透测试的目的和总体目标• 确定渗透测试的频率	华为云建立了渗透测试与漏洞扫描管理规定，明确了华为云平台开展渗透测试的目的、频率以及应遵循的安全要求，规范渗透测试行为，确保渗透测试活动合规与受控。	客户应制定渗透测试管理规范，规范渗透测试行为。
4.16. 2	定义{渗透测试}过程，包括渗透测试的范围和频率（例如每季度至少对关键信息资产进行一次渗透测试），使用标准方法识别未知漏洞（例如灰盒测试、白盒测试）。	华为云每半年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平台范围内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，渗透测试报告及跟进情况会通过内部审计以及外部认证机构核查。	客户应明确渗透测试的范围和频率，至少每季度对关键信息资产进行一次渗透测试。

4.16.3	根据所使用的渗透测试方法，使用[漏洞报告]作为输入来指导渗透测试。	华为云在进行渗透测试的过程中，会利用漏洞报告中已知的漏洞开展测试。	客户应使用漏洞报告作为输入来指导渗透测试。
4.16.4	向相关部门报告[渗透测试报告]，以在适用时触发补救措施[补丁管理]。	渗透测试发现的漏洞和风险通知到安全运维团队，由其拉通实施人员、业务团队、专家组织漏洞风险评估和制定处置计划，跟踪漏洞和风险闭环处理。渗透测试活动需形成正式的渗透测试报告，并向业务领域和上级主管部门进行结果汇报。	客户应将渗透测试的结果与相关人员报告并实施补救措施。
4.16.5	持续审查和优化[渗透测试要求]以及进行渗透测试所用的方法和相关流程。	华为云每年会对建立的渗透测试与漏洞扫描管理相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对渗透测试的网络安全要求进行审查和更新。

7.5 物理安全

“物理安全”要求客户制定并实施完善的物理和环境安全防护策略、规程和措施，以防止物理和环境潜在危险以及非授权访问。控制要求及华为云的实践方式如下：

7.5.1 安全设备和区域

保护信息资产免受物理损坏和威胁。

编号	具体控制要求	华为云的内部实践
5.1.1	定义[安全设备和区域的要求]考虑以下因素： <ul style="list-style-type: none">• 保护设备和物理设施• 交货和装载区• 设备运输	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。华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。
5.1.2	定义安全边界（考虑 [资产管理要求]）以保护包含敏感或关键信	华为云通过门禁控制系统，严格审核人员出入权限。 华为云要求来访者必须由内部人员全程陪同，并且只能在一般限制区域活动。华为云对于生产及非生产环境使

	息资产的物理设施（例如办公室、房间、数据中心、地面站点和电信处理设备）。	用物理和逻辑隔离手段。 在数据中心设计施工和运营时，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。						
5.1.3	确保设备位于适当的安全区内，并在非运行时间内储存在安全的物理设施中。	华为云制定了机要设备与介质管理相关规定，对设备的安置、保护、进出等均做出要求并制定操作流程。 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。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。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，确保非授权人员不可访问数据中心。						
5.1.4	保护可能被未经授权人员用于进入组织场所的交付/装载区域（例如，在可能的情况下对进出货物进行物理隔离）。	华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。						
5.1.5	保护设备免受环境威胁、危险和未经授权的访问造成的损坏。此外，为保护设备，应考虑以下因素：	<table border="1"><tr><td>电源故障和中断（由配套公共设施故障引起）</td><td>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)，提供短期备用电力供应。</td></tr><tr><td>确保电缆不受拦截、干扰或损坏，并进行适当的电缆管理（如电缆标签、颜色代码）</td><td>华为云数据中心选址时会考虑避开强电磁场干扰。华为云机房建设时规定用于任何网络布线和外接设备必须使用安全的导管和防篡改硬件。光纤电缆等通信设备穿过公开访问的区域时，管道和桥架会设置为金属材质，全程覆盖保护电缆，在管内或线槽铺设，并设置了漏电检测装置。</td></tr><tr><td>根据制造商规定的要求操作设备，并控制工作环境（例如温度、湿度、空气质量、水和光线）</td><td>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。</td></tr></table>	电源故障和中断（由配套公共设施故障引起）	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)，提供短期备用电力供应。	确保电缆不受拦截、干扰或损坏，并进行适当的电缆管理（如电缆标签、颜色代码）	华为云数据中心选址时会考虑避开强电磁场干扰。华为云机房建设时规定用于任何网络布线和外接设备必须使用安全的导管和防篡改硬件。光纤电缆等通信设备穿过公开访问的区域时，管道和桥架会设置为金属材质，全程覆盖保护电缆，在管内或线槽铺设，并设置了漏电检测装置。	根据制造商规定的要求操作设备，并控制工作环境（例如温度、湿度、空气质量、水和光线）	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。
电源故障和中断（由配套公共设施故障引起）	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)，提供短期备用电力供应。							
确保电缆不受拦截、干扰或损坏，并进行适当的电缆管理（如电缆标签、颜色代码）	华为云数据中心选址时会考虑避开强电磁场干扰。华为云机房建设时规定用于任何网络布线和外接设备必须使用安全的导管和防篡改硬件。光纤电缆等通信设备穿过公开访问的区域时，管道和桥架会设置为金属材质，全程覆盖保护电缆，在管内或线槽铺设，并设置了漏电检测装置。							
根据制造商规定的要求操作设备，并控制工作环境（例如温度、湿度、空气质量、水和光线）	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。							

	防止未经授权的访问（例如通过闭路电视监控）	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。
	桌面清理和屏幕清理政策（例如，将存储在文件上的敏感信息锁定在安全的地方，在不使用或无人值守时锁定计算机和/或终端的屏幕）	华为云制定并实施办公场所安全管理规定，对员工的安全责任与行为规范提出要求，制定政策和程序确保无人值守的工作区没有公开可见的敏感的文档。同时通过意识教育普及、宣传活动开展、BCG 及承诺书签署三个方面开展安全意识教育。
5.1.6	在运输过程中保护设备，同时考虑评估到的风险、移动过程中的安全性	华为云制定了存储介质及设备进出机房管理规定，要求存储介质及设备进出机房前需进行登记并得到授权。物理存储介质进出机房时均会进行数据防泄漏管理，并对数据擦除、报废清退流程进行规定，减少可能存在的数据泄露损失。
5.1.7	持续审查和优化 [安全设备和区域的要求]。	华为云每年会对建立的物理与环境保护相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。

7.5.2 物理访问管理

管理对承载信息资产的设施的物理访问，以防止未经授权的访问。

编号	具体控制要求	华为云的内部实践
5.2.1	定义[物理访问管理的要求]，考虑以下内容： <ul style="list-style-type: none">• 物理访问授权和控制• 监控物理访问	华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。 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。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。
5.2.2	创建和批准有权访问组织设施的	华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设

	个人的[物理访问控制列表]，并颁发适当的授权凭证。	备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。 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。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。
5.2.3	定义和实施{物理访问管理}流程以授予和管理对物理设施的访问（例如安全密钥）。	华为云制定了机要设备与介质管理相关规定，对设备的安置、保护、进出等均做出要求并制定操作流程。 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。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。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，确保非授权人员不可访问数据中心。
5.2.4	为访客建立物理入口控制（例如，向访客提供安全徽章并监控异常活动）。	华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。 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。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。
5.2.5	持续审查有权访问设施的个人的[物理访问控制列表]，并在不再需要访问时将其从列表中删除。	华为云通过门禁控制系统，严格审核人员出入权限。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，确保非授权人员不可访问数据中心。
5.2.6	定期查看物理访问日志，查看可疑活动[日志和监控]。	华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。 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。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。
5.2.7	持续审查和优化	华为云每年会对建立的物理与环境保护相关规范和策略

	[物理访问管理要求]以及用于处理物理访问管理的控制的有效性。	流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。
--	--------------------------------	---

7.5.3 环境保护

保护信息资产免受环境威胁。

编号	具体控制要求	华为云的内部实践
5.3.1	定义[环境保护要求]，考虑以下因素： • 确定针对内部和外部环境威胁的物理保护措施	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，确保物理保护措施免受内外部环境的威胁。
5.3.2	实施物理保护措施（例如部署和维护火灾探测和灭火设备/系统）以防止内部（例如事故、电源故障、由配套公共设施故障引起的其他中断）和外部环境威胁和危害（例如自然灾害）。	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，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（如火灾、电磁泄露等）和非授权访问，而且提供了足够的物理空间、电源容量、网络容量、制冷容量，以满足基础设施快速扩容的需求。同时，华为云运维运营团队严格执行访问控制、安保措施、例行监控审计、应急响应等措施，以确保华为云数据中心的物理和环境安全。
5.3.3	持续审查和优化[环境保护要求]以及针对紧急情况制定的控制措施的有效性。	华为云每年会对建立的物理与环境保护相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。

7.5.4 场外资产

保护组织场所外的信息资产免受物理和环境威胁。

编号	具体控制要求	华为云的内部实践
5.4.1	定义[场外资产要求]，考虑以下因素：	华为云制定并实施办公计算机安全管理规定，明确办公资产使用人有义务确保所使用资产的安全，并对使用状况负责。员工携带办公便携机外出时将其随身携带或妥善存放，确保便携机中所存储华为信息的安全。如办公

	<ul style="list-style-type: none"> • 保护安装在场外场所的设备和物理设施 • 互联电信服务 	计算机丢失或被盗，员工将及时报告。
5.4.2	实施适当的安全措施，以保护安装在场外场所（如备用工作场所、共同场所）的组织设备，并确保场外场所得到有效保护（如免受物理和环境威胁）。	华为云制定并实施办公计算机安全管理规定，明确办公资产使用人有义务确保所使用资产的安全，并对使用状况负责。员工携带办公便携机外出时将其随身携带或妥善存放，确保便携机中所存储华为信息的安全。如办公计算机丢失或被盗，员工将及时报告。
5.4.4	持续审查和优化[场外资产要求]以及网络安全控制的有效性，以保护场外资产。	华为云每年会对建立的物理与环境保护相关规范和策略流程进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。

7.6 第三方安全

“第三方安全”为客户实施业务外包提供了指引。对客户的控制要求覆盖服务供应商能力、合同和协议、客户数据机密性、云服务的使用等领域。相关控制要求及华为云的实践方式如下：

7.6.1 云服务

确保其云服务提供商签订并应用网络安全要求。

编号	具体控制要求	华为云的内部实践	客户的职责
6.1.1	<p>定义[云服务要求]，考虑以下因素：</p> <ul style="list-style-type: none"> • 云风险评估 • 确定云提供商预期的网络安全要求 • 服务水平协议 	华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供的服务内容和服务水平，以及华为云的职责。华为云作为云服务提供商，确保各项云技术的安全开发、配置和部署以及所提供的云服务的运维运营安全。	客户应建立云计算服务相关的网络安全要求，确保在云上的组织的信息和技术资产的安全。
6.1.2	在采用云服务之前（或在相关立法和监管要求发	华为云会遵从与客户订立的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评	客户应在采用云服务之前对该云提供商进行风险

	生变化的情况下)，根据[网络安全风险评估要求]进行风险评估，以确保与使用云服务相关的风险得到适当解决。	估。	评估。
6.1.3	确定云服务提供商应遵守的网络安全要求（例如，在云中托管之前对数据进行分类，保护组织数据的机密性、完整性和可用性，将云中的组织数据与云中的其他数据隔离）{信息分类}。	华为云作为云服务提供商，遵守客户提出的网络安全要求，确保各项云技术的安全开发、配置和部署以及所提供云服务的运维运营安全。华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。	客户应明确云服务提供商应遵守的网络安全要求。客户在使用云服务之前，需要对其数据进行分类，并进行风险分析，再根据风险分析结果，明确防护数据的存储位置、存储服务和安全防护措施。
6.1.4	与云服务提供商建立服务水平协议 (SLA)，至少考虑以下方面：		
	预定义的网络安全要求。	华为云恪守“不碰数据”底线，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令，并严格遵守《CRF》所述的网络安全原则。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。 华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。	客户应在与云服务提供商签订的合同或协议中明确云服务提供商须遵守组织政策和程序、法律法规的要求。
	发生网络安全事件时的沟通程序。	针对影响客户的安全事件，华为云建立了完善的事件通告机制。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施	客户应在与云服务提供商签订的合同或协议中明确发生网络安全事件时的沟通程序。

		等。在事件解决后，会根据具体情况向客户提供事件报告。	
	终止云服务的权利（以可用格式返回组织数据，不可逆转地删除组织数据）。	在客户确认删除数据后，华为云会对指定的数据及其所有副本进行全面的清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。	客户应在与云服务提供商签订的合同或协议中明确在服务结束时使用安全措施删除组织的数据。在服务协议终止时，客户可通过华为云提供的云数据迁移服务（CDM），将内容数据从华为云中迁移出去，如迁移至本地数据中心。
6.1.5	确保组织数据的托管和存储站点位于沙特阿拉伯王国。	华为云会将组织数据的托管和存储站点部署在沙特阿拉伯王国境内。	客户应确保组织的信息托管和存储位于沙特阿拉伯王国境内。
6.1.6	审计、审查和监控云服务提供商是否遵守合同义务。	华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。	客户应审查和监控云服务提供商是否遵守合同义务。
6.1.7	持续审查和优化[云服务的要求]以及选择云服务所涉及的程序和预期的网络安全要求。	华为云作为云服务提供商，每年会对建立的信息安全管理进行审阅和更新，同时华为云网络安全与隐私办公室定期对策略的执行情况进行定期的审视，确保安全治理的策略、标准、规范和具体措施在各业务领域的流程落地。	客户应根据计划的频率定期对使用云计算有关的网络安全要求进行审查和更新。

7.6.2 外包服务

确保向组织提供外包服务的第三方签订并实施网络安全要求。

编号	具体控制要求	华为云的内部实践	客户的职责
6.2.1	定义[外包服务要求]，考虑以下因素： •将服务外包给第三方的风险评估	华为云提供了线上的《华为云用户协议》以及华为云《云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定	客户应在与第三方签订的合同和协议中明确网络安全要求，降低第三方访问组织资产的相关风

	<ul style="list-style-type: none">•满足第三方供应商的网络安全要求•服务水平协议	<p>制化。</p> <p>在华为云内部，华为云建立了正式的采购审核流程，在供应商入场前，华为云要求须同供应商签署合同、服务协议及保密协议。合同与服务协议中明确了双方的责任和义务、服务内容及服务水平等要求，同时通过保密协议对违反保密性的条款进行了约束。华为云法务部门每年会对采购保密协议进行审阅及更新，以确保采购保密协议可以持续满足业务对供应商的管理要求。</p>	险。
6.2.2	在将任何服务外包给第三方供应商之前（或在相关立法和监管要求发生变化的情况下），根据[网络安全风险评估要求]进行风险评估，以确保与使用外包相关的风险得到适当解决。	<p>华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。</p> <p>在华为云内部，华为云已建立供应商选择和监督体系，并规范了研发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。</p>	客户应建立风险评估框架，定期评估外包服务的风险。
6.2.3	确定第三方供应商应遵守的网络安全要求（例如保密条款）。	<p>华为云恪守“不碰数据”底线，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令，并严格遵守《CRF》所述的网络安全原则。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。</p> <p>在华为云内部，华为云在引入供应商时会与其签署保密及服务水平协议，协议中包含对于供应商的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。供应商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。针对华为云的供应商，华为云会定期对其服务的安全合规性进行评估，对其可以提供的用户个人信息安全性保护能力进行评估。</p>	客户应明确第三方须遵守组织政策和程序、法律法规的要求。
6.2.4	与第三方服务供应商建立服务水平协议，至少考虑以下几点：		

	<p>预定义的网络安全要求。</p>	<p>华为云恪守“不碰数据”底线，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守法律法规或政府机关的约束性命令，并严格遵守《CRF》所述的网络安全原则。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。</p> <p>在华为云内部，华为云在引入供应商时会与其签署保密及服务水平协议，协议中包含对于供应商的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。供应商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。针对华为云的供应商，华为云会定期对其服务的安全合规性进行评估，对其可以提供的用户个人信息安全性保护能力进行评估。</p>	<p>客户应明确第三方须遵守组织政策和程序、法律法规的要求。</p>
	<p>发生网络安全事件时的沟通程序。</p>	<p>针对影响客户的安全事件，华为云建立了完善的事件通告机制。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。</p>	<p>客户应在与第三方提供商签订的合同或协议中明确发生网络安全事件时的沟通程序。</p>
	<p>终止与第三方提供商的合同义务的权利。</p>	<p>在客户确认删除数据后，华为云会对指定的数据及其所有副本进行全面的清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。</p> <p>在华为云内部，华为建立了完善的供应商管理流程，在采购前会对供应商的网络安全能力进行评估，必要时会对供应商执行尽职调查，并制定综合采购变更管理规定及流</p>	<p>客户应在与第三方提供商签订的合同或协议中明确终止与第三方提供商的合同义务的权利。</p> <p>在服务协议终止时，客户可通过华为云提供的云数据迁移服务（CDM），将内容数据从华为云中迁移出去，如迁移至本地数据中心。</p>

		程，按照管理规定严格管理供应商服务的变更，明确其终止与第三方供应商的合同的权利。	
6.2.5	审计、审查和监控第三方供应商是否遵守合同义务。	<p>华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。</p> <p>在华为云内部，华为云已建立供应商选择和监督体系，通过合同签订前的尽职调查以及合同签订后的定期评估来管理供应商对华为云具体的要求和合同义务的符合性。</p>	客户应审查和监控第三方服务提供商是否遵守合同义务。
6.2.6	确保与在关键系统上工作的第三方人员签订合同时对其进行筛选。	<p>华为云会遵从与客户订的协议中约定的要求，华为云会安排专人积极配合客户对华为云的监督和风险评估。</p> <p>在华为云内部针对外部人员，在聘用外部人员前对其进行背景调查，华为云接口部门在与之签署的合同或协议条款中明确约定对外部人员及所属公司的信息安全管理要求，以及信息安全违规处罚措施。</p>	客户应确保与在关键系统上工作的第三方人员签订合同时对其进行筛选。
6.2.7	持续审查和优化[外包服务要求]以及选择第三方服务供应商所涉及的程序和预期的网络安全要求。	华为云法务部门每年会对采购保密协议进行审阅及更新，以确保采购保密协议可以持续满足业务对供应商的管理要求。	客户应根据计划的频率定期审查和更新与第三方签订的合同和协议的网络安全要求。

8 结语

本文描述了华为云为客户提供 的云服务如何遵从沙特阿拉伯网络安全监管要求，并表明沙特阿拉伯国家网络安全局（NCA）与通信、空间和技术委员会（CST）发布的重点监管要求，有助于客户详细了解华为云如何遵从沙特阿拉伯网络安全监管要求，让客户安全、放心地通过华为云服务存储、处理客户内容数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合沙特阿拉伯网络安全监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

本文仅供参考，不具备法律效应或构成法律建议。客户应酌情评估自身使用云服务的情况，并确保在使用华为云时对相关沙特阿拉伯网络安全监管要求的遵从性。

9 历史版本

日期	版本	描述
2023 年 12 月	1.1	例行刷新
2022 年 7 月	1.0	首次发布