华为云土耳其网络安全监管遵从性指南

文档版本 1.0

发布日期 2026-07-13



华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2026。 保留一切权利。

非经本公司书面许可，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


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 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 4
3 华为云责任共担模型 7
4 华为云全球基础设施 9
5 华为云如何遵从及协助客户满足《网络安全法》的要求 10
6 华为云如何遵从及协助客户满足《信息通信指南》的要求 14
6.1 网络和系统安全 14
6.2 应用程序和数据安全 39
6.3 人员安全 40
6.4 物理场所的安全 42
6.5 个人数据的安全 44
6.6 云计算安全 46
7 华为云为客户提供的安全与隐私保护相关的云服务 51
8 结语 55
9 版本历史 56

1 概述

1.1 背景与发布目的

随着信息科技的迅猛发展，越来越多的组织正积极寻求业务转型，希望借助人工智能、大数据、云计算等先进技术来降低成本、提升运营效率，并实现业务模式的创新。然而，技术的快速演进也带来了网络安全、数据隐私和内容合规等新的挑战。为了规范信息科技的运用，土耳其网络安全局发布了一系列法律和监管要求，针对网络安全管理、应用实施、数据保护等方面提出了详细的合规要求。

华为云作为云服务提供商，致力于协助客户满足这些监管要求，持续为客户提供遵从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土耳其网络安全监管要求，详细阐述华为云将如何协助其满足这些监管要求。

1.2 网络安全监管要求简介

土耳其网络安全局（Türkiye Cyber Security Presidency）是土耳其网络安全治理的核心领导机构。其职责包括拟定国家网络安全政策、界定国家级安全等级标准，是集中管理数字化转型（电子政务）、网络安全、国家技术、大数据和人工智能的部门。

- **《网络安全法》 (Cybersecurity Law)**：总统府于 2025 年 3 月 12 日发布了网络安全法。该法律体系定义了内容提供商、托管提供商、访问提供商及社交网络提供商的法律义务，要求其对非法内容承担过滤或删除责任。赋予监管机构在无需司法裁决的情况下，针对危害国家安全或公共秩序的内容采取带宽限制（Throttling）、封锁或行政处罚的权力。
- **《信息与通信安全指南》**：土耳其总统府于 2019 年 7 月 5 日发布《关于信息和通信安全措施的第 2019/12 号总统通告》旨在制定一系列提高关键数据安全性的措施要求。 2020 年 7 月 10 日根据国家、国际标准以及信息安全标准制定《信息与通信安全指南》。本指南确定了公共机构和组织以及提供关键基础设施服务的企业要执行的最低安全措施，同时确保可能威胁国家安全或导致公共秩序恶化的关键信息和数据的安全。

土耳其信息与通信技术管理局（BTK，Information and Communication Technologies Authority）是土耳其电信与网络安全治理的核心执行与监管机构。其职责包括拟定通信与网络安全政策、界定国家级网络安全标准、颁发电信许可并进行市场监管，是集

 版权所有 © 华为云计算技术有限公司

中管理电信基础设施、频谱分配。BTK 之前的网络安全应急响应（USOM）和数字化转型职责已移交给网络安全局。

- **《电子通信法 (Elektronik Haberleşme Kanunu)》**：该法于 2008 年 11 月 10 日正式发布实施，是土耳其电子通信领域的基石性法律，旨在促进市场竞争、保护消费者权益并确立监管框架。它赋予了信息与通信技术管理局（BTK）核心监管权，规定了电信运营商的准入许可、频谱分配以及基础设施建设标准。同时，该法对保障国家安全、维护公共秩序以及紧急状态下的通信管制奠定了法律基础。《信息与通信安全指南》已包含并细化相关要求，不再单独分析，详情见本白皮书第 6 章。

- **《电子通信安全条例 (Elektronik Haberleşme Güvenliği Yönetmeliği)》**：该条例由土耳其信息与通信技术管理局（BTK）于 2014 年 7 月 13 日正式发布实施。该条例是针对电子通信网络和物理基础设施安全的专项行政法规。它明确要求电信运营商和关键服务提供商必须建立完善的网络安全防御体系，制定风险管理与应急响应预案。条例重点规范了网络攻击的防范、安全漏洞的审查以及数据传输的机密性，旨在确保土耳其国家通信网络免受恶意破坏，保障社会平稳运行。《信息与通信安全指南》已包含并细化相关要求，不再单独分析，详情见本白皮书第 6 章。

- **《电子通信行业信息系统规定 (Elektronik Haberleşme Sektöründe Bilgi Sistemleri Yönetmeliği)》**：该规定由土耳其信息与通信技术管理局（BTK）于 2016 年 7 月 13 日正式发布实施。该规定规范确定和监督电子健康辅助设施和电子通信基础设施设施最低要求的程序和原则。《信息与通信安全指南》已包含并细化相关要求，不再单独分析，详情见本白皮书第 6 章。

1.3 名词定义

- **华为云**

  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。

- **信息系统**

  收集、处理、储存、分配和利用信息的人力资源、业务活动和流程，以及与之互动的信息技术。

- **网络事件**

  侵犯信息系统或数据的保密性、完整性或可访问性的事件。

- **网络安全**

  保护构成网络空间的信息系统免受攻击，以及在这种环境中处理的数据的机密性；确保完整性和可访问性，检测攻击和网络事件；所有活动，包括启动对这些检测的反应和警报机制，然后恢复到网络事件发生前的状态。

- **关键基础设施**

  托管信息系统的基础设施，当其处理的信息/数据的机密性、完整性或可访问性受到损害时，可能会导致生命损失、大规模经济损失、国家安全漏洞或公共秩序中断。

 版权所有 © 华为云计算技术有限公司

- **关键基础设施部门**

  指国家网安全战略确定的关键基础设施部门。

 版权所有 © 华为云计算技术有限公司

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 系统的建设和运营经验，对华为云各项服务的集成、运营及维护进行主动管理，并持续改进。截至目前，华为云已获得众多全球性、区域性和行业特定的安全合规的权威认证，全力保障客户部署业务的安全。

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

华为云部分标准类认证/鉴证示例：

认证	描述
ISO 27001	ISO 27001是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。
ISO 27017	ISO 27017是针对云计算信息安全的国际认证。ISO 27017的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO 27018	ISO 27018是专注于云中个人数据保护的国际行为准则。ISO 27018的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。
ISO 42001	ISO/IEC 42001是全球首个人工智能管理体系标准，由国际标准化组织(ISO)和国际电工委员会(IEC)联合发布，该标准提供了一个可认证的人工智能管理体系（AIMS）框架，为组织建立、实施、维护和持续改进人工智能管理体系提供要求和指南，旨在帮助组织和社会负责任地开发、提供和使用AI系统，并从人工智能中受益。
TL 9000& ISO 9001	ISO 9001是ISO 9000族标准所包括的一组质量管理体系核心标准之一，用于证实组织具有提供满足顾客要求和适用法规要求的产品的能力。 TL 9000是一个建立在ISO 9001基础上的，由全球电信业优

 版权所有 © 华为云计算技术有限公司

认证	描述
	质供应商联盟（QuEST Forum）针对全球信息和通讯技术（ICT）行业特定设计的、为ICT产品和服务供方提供的一套通用的质量管理体系要求。它包括了ISO 9001的所有要求，ISO 9001将来的任何改动也会导致TL9000的改动。 华为云取得了ISO 9001 / TL9000认证证书，表明华为云可以为您提供更快，更好和更具成本效益的服务。
ISO 20000	ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的IT服务来满足客户和业务的需求。
ISO 22301	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	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。
ISO 27701	ISO 27701规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过ISO 27701表明了其在个人数据保护具有健全的体制。
BS 10012	BS 10012是BSI发布的个人信息数据管理体系标准，BS 10012 认证的通过表明华为云在个人数据保护上拥有完整的体系以 保证个人数据安全。
ISO 29151	ISO 29151是国际个人身份信息保护实践指南。ISO 29151的通 过，表明华为云实施国际认可的个人数据处理的全生命周期 的管理措施。
PCI DSS	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。
PCI 3DS	PCI 3DS标准，旨在保护执行特定3DS功能或者存储3DS数 据的3DS环境，支持3DS的实施。PCI 3DS的评估对象为3D 协议执行环境，包括访问控制服务器、目录服务器或3DS服 务器功能；以及3D执行环境内和连接到环境所需要的系统组件，如防火墙、虚拟服务器、网络设备、应用等；除此之外，还会评估3D协议执行环境的过程、流程、人员管理等。
ISO 27799	ISO/IEC 27799是专注于医疗行业的信息安全管理体系，为医疗行业和其相关机构提供了关于如何更好地保护个人健康信

 版权所有 © 华为云计算技术有限公司

认证	描述
	息的保密性、完整性、可审计性和可用性的指导。 华为云是全球首个获得该认证的云服务商，表明华为云对医疗行业的理解和实践，对医疗行业信息安全的防护能力得到国际权威认可，能够更可靠的保障您的信息安全。
ISO 27034	ISO/IEC 27034是国际标准化组织ISO通过的第一个关注建立安全软件程序流程和框架的标准，它清晰地定义了实际应用中软件系统面临的风险，同时为不同类型的软件开发组织提供了一套可以灵活应用的方法。华为云是全球首家获得ISO/IEC 27034认证的云服务提供商，表明华为云具备在云服务中保持持续安全和合规的能力。
SOC 审计报告	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。

 版权所有 © 华为云计算技术有限公司

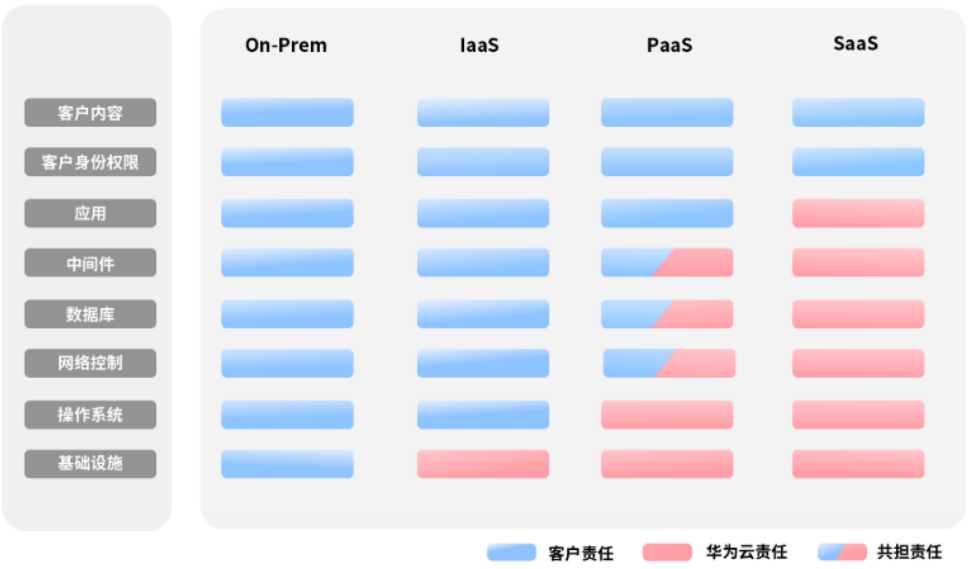
3 华为云责任共担模型

客户在云上业务的安全性与合规性是华为云与客户的共同责任。与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。也正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与客户共同努力。

云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如下图所示，客户可以基于自身的业务需求选择不同的云服务类别（例如 IaaS、PaaS、SaaS 服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

在监管要求可能适用于客户内容的情况下，“责任共担”模型帮助华为云和客户双方理解各自角色以及责任。

图 3-1 华为云责任共担模型



华为云的责任：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络

 版权所有 © 华为云计算技术有限公司

等）、虚拟化平台及云服务组成。在 PaaS、SaaS 场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。

客户的责任：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转 移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

在 On-prem 场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。

在 IaaS 场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。

在 PaaS 场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。

在 SaaS 场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

 版权所有 © 华为云计算技术有限公司

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。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**”。

图 4-1 土耳其地理区域（Region）和可用区（AZ）示例



 版权所有 © 华为云计算技术有限公司

5 华为云如何遵从及协助客户满足《网络安全法》的要求

《网络安全法》体系定义了内容提供商、托管提供商、访问提供商及社交网络提供商的法律义务，要求其对非法内容承担过滤或删除责任。赋予监管机构在无需司法裁决的情况下，针对危害国家安全或公共秩序的内容采取带宽限制（Throttling）、封锁或行政处罚的权力。

以下内容将总结《网络安全法》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。

编号	具体控制要求	客户关注点	华为云的应答
第四条	1）确保网络安全的基本原则如下： e) 所有公共机构和组织以及自然人和法人均有责任实施网络安全政策和战略，并采取必要措施防止或减轻网络攻击的影响。 f) 在网络安全流程的实施过程中，问责制至关重要。 g) 网络安全政策和战略制定工作采用持续改进的方法进行。	客户应 1.确保系统、服务或产品符合国家安全要求。 2.保护关键基础设施和信息系统，并创建一个安全的网络空间。 3.建立并实施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。 4.在服务和产品的整个生命周期中实施网络安全措施。 5.保证网络安全领域合格人力资源的能力和素质。 6.确保符合隐私保护和其他方面的国家原则。	1.华为云遵守适用的土耳其法律法规或政府机关的约束性命令，提供的服务和产品均符合要求。华为云业务的开展遵循华为公司“一国一策，一客一策”的战略，在遵从客户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、生态和等方面建立并管理完善、高可信、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放合作的方式，共同应对云安全挑战，助力客户的安全需求。 2.客户可依赖华为云在土耳其的数据中心集群的多可用区（AZ）架构实现其业务系统的容灾和备份，华为云在土耳其伊斯坦布尔有三个可用区，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从相关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。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。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			3.根据ISO27001标准，华为云构建了完善的信息安全管理体系，制定了华为云的整体信息安全战略，明确了信息安全管理机构的结构和职责、信息安全系统文件的管理方法、关键方向和目标，包括资产安全、访问控制、密码学、物理安全、运营安全、通信安全、系统开发安全、供应商管理、信息安全事件管理和业务连续性。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。此外，华为云建立了严密的安全责任体系，贯彻违规问责机制。 4.华为云明确了责任共担模型，无论使用哪一项华为云服务，租户始终是其数据的所有者和控制者。租户负责各项具体的数据安全配置，对其保密性、完整性、可用性以及数据访问的身份验证和鉴权进行有效保障。详情可参考华为云责任共担模型。 5.华为云在服务和产品的整个生命周期中实施网络安全措施，包含产品开发，测试，上线实施，运营维护，下线阶段。华为云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，确保信息安全在信息系统安全生命周期中得到设计和实现。 6.华为云制定了完善的安全意识培训计划，在员工入职、在岗、转岗等环节纳入多种形式的安全意识培训，确保员工行为符合所有法律、政策、流程以及华为商业行为准则的要求。此外，华为云建立了严密的安全责任体系，贯彻违规问责机制，并通过意识培训让员工知晓违规行为可能导致的处分。 7.更多关于华为云如何满足土耳其隐私合规要求可以参见华为云官网已发布的《土耳其隐私遵从性指南》。 8.作为云服务商，华为云： 1) 华为云提供符合本地化部署与安全合规要求的产品。华为云致力于为客户提供既满足本地化部署需求，又具备高安全保障能力的云产品。客户可在本地数据中心享受与公有云一致的创新迭代速度。在产品安

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			全方面，华为云视安全为基线，构建安全可信的云服务，通过了ISO 27001、CSA STAR等30+项权威认证，覆盖数据存储、传输、处理全流程。 2) 为协助客户满足政府安全监管要求，华为云提供一系列符合国际与政府标准的安全产品。华为云深知政府及关键行业客户在安全合规方面的严格要求，因此提供了一整套符合土耳其内外权威标准的安全产品与服务。这些产品覆盖网络安全、数据安全、安全管理、应用安全等多个领域，包括但不限于：**Web应用防火墙（Web Application Firewall，简称WAF）**、**密码安全中心（Data Encryption Workshop，简称DEW）**等。 3) 更多保障与增强安全合规的产品或服务信息，客户可登录华为云官网，查阅最新的安全认证全景图、产品信息以及行业解决方案详情，以获取全面的安全合规支持。
第七条	b) 为维护国家安全、公共秩序或保障公共服务正常运作，采取法律规定的网络安全措施，并立即向总统府报告其在服务领域内发现的任何漏洞或网络安全事件。 c) 从总统府授权和认证的网络安全专家、制造商或公司采购网络安全产品、系统和服务，供公共机构和组织以及关键基础设施使用。 c) 网络安全公司须经认证、授权和文件编制，方可开始运营。公司必须在现有法规框架内获得总统府的批准。	客户应立即向总统府报告其在服务领域内发现的任何漏洞或网络安全事件。网络安全公司须获得总统府的认证、授权和文件编制，方可开始运营。	1.华为云参照ISO 27001、ISO 20000、CSA STAR等众多的国际及行业标准，构建并实施了一套完善的信息科技风险管理体系，涵盖了IT治理/管理、信息系统开发和获取、IT运营、通信网络、信息安全等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。 2.为配合客户满足监管要求，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。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
第八条	1）总统府在履行本法规定的职责时，如认为有必要，可对本法范围内的任何行为或交易进行审计；为此，总统府可进行或委托进行现场检查。审计范围涵盖本法范围内的机构、组织及其他相关自然人和法人根据本法规定开展的活动和交易。总统府工作人员、经授权和认证的独立审计师和独立审计公司均有权进行审计。此项权力由总统任命的人员行使。对公共机构、组织和关键基础设施的审计由总统府工作人员进行或陪同进行。 （2）总统府确定审计活动的重要性原则和优先原则、风险评估所考虑的标准以及实施原则。审计活动应按照在重要性原则、优先原则和风险评估范围内制定的方案进行。如有必要审查方案之外的事项，总统府可要求在方案之外进行审计。 （3）民事当局、执法人员以及其他公共机构的官员和工作人员有义务向负责进行调查或审计的人员提供各种便利和协助。 （4）受命进行审计的人员有权在其审计活动范围内检查电子数据、文件、电子基础设施、设备、系统、软件和硬件，并可复制、数字化或抽取样本，要求就相关事项作出书面或口头解释，编制必要的会议记录，并检查设施及其运行情况。被审计方有义务在规定的期限内保持相关设备、系统、软件和硬件处于可供审计的状态，提供必要的审计基础设施，并采取必要措施确保其正常运行。	客户应配合行政部门对金融机构的审计权。	1.客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。 2.华为云会安排专人积极配合监管机构发起的审计要求。此外，华为云已通过ISO 27001、ISO 27017、ISO 27018、SOC、CSASTAR等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。

版权所有 © 华为云计算技术有限公司

6 华为云如何遵从及协助客户满足《信息通信指南》的要求

《信息通信安全指南》的目的是确定公共机构及提供关键基础设施服务的企业执行最低安全措施，以减少和消除信息安全风险，并确保可能威胁国家安全或导致公共秩序恶化的关键信息和数据的安全。

以下内容将总结《信息通信安全指南》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。

6.1 网络和系统安全

6.1.1 威胁和漏洞管理

编号	具体控制要求	客户关注点	华为云的应答
3.1.3.1	应使用自动软件更新工具检查所有系统上的软件，以确保它们满足当前的业务要求，并以软件制造商提供的最稳定和最新的安全版本运行。在无法使用自动软件更新工具的情况下，应由专家定期进行必要的手动检查。	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。对所有系统上的软件进行检查，确保都是以最稳定和最新的安全版本运行。	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。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.3.3	应制定策略和流程，及时检测企业应用程序、企业网络和系统组件的安全漏洞。漏洞和补丁管理的变更应通过定义的变更管理流程以受控方式进行。	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（Image Management Service，简称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。 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。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。 同时，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。
3.1.3.8	应使用自动软件更新工具检查操作系统的更新和补丁，尤其是安全更新，是否考虑了制造商报告的最稳定、最新和可靠的版 本。	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。同时，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。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.3.9	1.使用符合安全内容自动化协议 (SCAP) 的漏洞扫描工具定期扫描公司网络中的所有系统（包括测试系统）。 2.定期扫描为漏洞扫描所创建账户的安全性。 3.漏洞扫描工具应生成安全报告，且未经授权不得访问。 4.为安全扫描创建的账户不得移作他用，并按照最小授权、无需知晓的原 则，通过授权保存相关访问记录。	客户应使用符合安全内容自动化协议(SCAP)的自动化漏扫工具对公司网络中的所有系统进行漏洞赛扫描，输出漏洞扫描报告。创建的漏洞扫描账号应符合最小授权、无需知晓的原则，并定期检查该账号的使用情况。 客户应保障漏洞扫描报告的安全性，控制漏洞报告的访问权限。	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。 除此之外，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。 华为云员工账号管理遵从公司用户账号权限管理规定。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。对账号进行分类管理并建立访问控制策略，相关文件均通过评审流程并发布。华为云根据不同业务维度和相同业务的不同职责，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。不同岗位的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 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。

 版权所有 © 华为云计算技术有限公司

6.1.2 恶意软件保护

编号	具体控制要求	客户关注点	华为云的应答
3.1.5.1	反恶意软件应用程序应在所有客户端和服务器系统中使用，并应确保反恶意软件应用程序中的最新补丁文件和签名数据库是最新的。反恶意软件应用程序的策略应集中管理。	客户应定义恶意软件处理的安全要求，应在所有客户端和服务器系统中使用防恶意软件程序，并采取措施防止用户停用或更改此软件。	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。

6.1.3 网络安全

编号	具体控制要求	客户关注点	华为云的应答
3.1.6.4	应使用黑名单或白名单来限制实体的网络访问。	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。	华为云提供的**虚拟私有云（Virtual Private Cloud，简称 VPC）**服务，实现不同区域之间网络隔离。VPC 可为租户构建出私有网络环境，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络 ACL 和安全组规则，对进出子网和虚拟机的网络流量进行严格的管控，满足租户更细粒度的网络隔离需求。 华为云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 -

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			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。 数据中心外网运维人员和内网运维人员对网络、服务器等设备的本地及远程操作全部集中管理，实现用户对设备资源操作管理的统一接入、统一认证、统一授权、统一审计。
3.1.6.5	公司的网络边界只有允许的源和允许的目的地才应使用允许的端口和协议传输流量。	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。客户应制定访问控制策略限制对组织网络的访问，限制对高危端口及高危协议的使用。	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）**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。 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。并且华为云在边界处部署了 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； 除此之外，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

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			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。
3.1.6.7	对于向互联网开放的服务，至少应采取以下措施，以防止其因可能的 DoS/DDoS 攻击而停止服务，并保证业务连续性。 在安全产品进行针对 DoS/DDoS 攻击的特定配置。 定期测试并持续改进/更新 DDoS 防护系统的能力。 如果提供商提供了 DDoS防护服务，从服务提供商处获得已按照上述要求提供服务的承诺，并在供货规格和合同中详细说明这些事项。	客户应确保对传入和传出流量进行控制，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。防御系统应定期审查，持续更新相关功能。从外部获取入侵防御系统服务时应与供应商明确规定服务要求。	客户可通过华为云 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。 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。
3.1.6.8	应防止从互联网不受控制地访问内部资源。如果需要从 Internet 访问内部资源，则应使用 VPN 技术。应确保远程访问是按照机构的政策和程序、在有限的时间和授权下进行的。	客户应制定并实施访问控制措施。	客户除了通过**统一身份认证服务（Identity and Access Management，简称IAM）**进行人员的身份和权限管理外，华为云还提供了加密传输的方式供客户自行选择，比如**虚拟专用网络（Virtual Private Network，简称VPN）**。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。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.6.17	应建立记录机制，以监控确定的源和目的地之间的所有网络流量。在需要时（安全漏洞、可疑网络流量等），机构应能够在确定的时间段内利用这些机制检查相关流量记录。	客户应制定监控机制，监控及分析确定的源和目的地之间的所有网络流量。	客户可使用华为云 Anti-DDoS 流量清洗服务，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。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。华为云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。其次，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。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。
3.1.6.19	应使用基于网络的入侵检测和防御系统来检测和阻止攻击。	客户可在网络边界部署入侵防御系统，以应对针对组织网络的内部和外部攻击。	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。 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。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.6.20	所有进出互联网的网络流量都必须在应用层进行过滤和身份验证，以防止未经授权的连接。	客户应对所有进出互联网的网络流量都必须在应用层进行过滤和身份验证，以防止未经授权的连接。	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（Web Application Firewall，简称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。 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。
3.1.6.28	应适当定位、测试并持续改进必要的结构（WAF、IPS、DDoS 等），以保护企业网络免受应用程序级攻击。如果服务提供商为此目的提供服务；应获得服务提供商的承诺，即按照上述条件提供服务，并应在供货规格和合同中明确这些问题。	客户应根据计划的频率定期对安全架构进行审查和更新。如果客户从服务提供商采购了相关安全服务，应与供应商签订的合同中约束供应商对安全架构及策略进行持续改进的责任。	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。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。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.6.33	加密网络设备应用于关键网络环境之间的通信。	在政府机构之间的关键网络之间进行信息或数据通信时，客户需要对敏感或重要的数据进行保护，并使用加密设备对通信内容进行加密，以保证机密性和安全性。	华为云制定了安全管理规定，明确了信息传输策略和流程，并制定了详细的控制要求。 在华为云的客户端和服务器之间、服务器之间通过公共信息通道传输数据的场景下，对传输中的数据进行如下保护：**虚拟专用网络（Virtual Private Network，简称VPN）** 用于在远程网络和租户**虚拟私有云（Virtual Private Cloud，简称VPC）**之间建立符合行业标准的安全加密通信通道，使租户现有的本地数据中心无缝扩展到华为云，同时保证端到端的数据机密 性。通过在传统数据中心和 VPC 之间建立基于 VPN 的通信通道，租户可以方便地使用云服务器、块存储等华为云资源。应用程序可以迁移到云端，可以启动额外的 Web 服务器，并可以扩展租户空间内的计算能力，从而建立企业混合云架构，同时还可以降低租户核心业务数据未经授权传播的风险。 目前，华为云采用 IPsec VPN 结合 IKE(Internet Key Exchange)技术，对数据传输通道进行加密，保证传输安全性。-应用层 TLS 和证书管理：华为云支持 REST 和 Highway 两种方式的数据传输。REST 模式是指服务作为 RESTful服务对外发布，发起方直接使用 HTTP客户端发起 RESTful API 进行数据传输。Highway 方式是通过高性能的华为私有协议建立通信通道，最适合对性能要求特别高的场景。REST 和Highway 两种模式都支持 TLS 1.2 协议，用于传输数据加密和基于 X.509证书的目标网站身份认证。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.6.17	应建立记录机制，以监控确定的源和目的地之间的所有网络流量。在需要时（安全漏洞、可疑网络流量等），机构应能够在确定的时间段内利用这些机制检查相关流量记录。	客户应制定监控机制，监控及分析确定的源和目的地之间的所有网络流量。	客户可使用华为云 Anti-DDoS 流量清洗服务，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。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。华为云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。其次，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。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。

6.1.4 防止数据泄露

编号	具体控制要求	客户关注点	华为云的应答
3.1.7.2	使用云服务时，应在服务规范和合同中明确数据访问、存储和使用范围内的安全问题。	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。客户应在合同中明确云服务提供商应遵守的在数据访 问、存储和使用范围内的安全职责。	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。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.7.8	应使用基于网络的数据泄露防护系统来控制和监控网络内的数据流，并监控未经授权的网络流量。	客户应部署数据泄露防护系统来控制数据流，并监控未经授权的网络流量。	客户可以采用华为云**数据库安全服务（Database Security Service，简称DBSS）**为数据库提供替身式防护。 DBSS 基于专利保护的反向代理模式以及机器学习机制，集数据脱敏、数据库防火墙和数据库审计功能于一体，一站式全方位保障云上数据库的安全。通过数据安全中心(DSC)客户可以对指定数据配置脱敏规则实现敏感数据静态脱敏，也可以使用数据动态脱敏的 API 接口实现数据的动态脱敏，全方位确保敏感信息不被泄露。在数据使用环节，客户可针对不同类型的敏感数据，使用不同的脱敏方式进行脱敏，敏感数据保护服务中已预置多种字符脱敏模板。 华为云高度重视用户的数据信息资 产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流 程，为用户提供最切实有效的数据保护能力，保证租户对其数据的隐私权、所有权和控制权不受侵犯。 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（Virtual Private Network，简称VPN）**：用于在远端网络和 **虚拟私有云（Virtual Private Cloud，简称 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。 华为云参考业界加密算法优秀实践，针对存储数据制定并实施了密码算法应用规范，对加密级别、加密方法进行了明确规

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			定。华为云根据规范，使用了 AES 强加密算法针对存储在云基础设施中的静态数据执行数据加密，有效保护云平台中的数据安全。 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。

6.1.5 保存和监测跟踪和审计记录

编号	具体控制要求	客户关注点	华为云的应答
3.1.8.1	所有系统和网络设备需要启动日志记录，应根据信息安全要求和相关立法将记录保存在设备或外部系统上可接受的时间段内，并应防止未经授权的访问和更改。记录应在规定的可接受保留期限届满时安全销毁。	客户应制定事件日志与监控的安全管理策略，并根据相关立法制定日志的留存机制，确保在留存期满后安全删除日志。	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。 华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，以确保支撑网络安全事件回溯和合规。该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超过 180 天，90 天内可以实时查询。
3.1.8.2	系统管理员、操作员和用户的活动应予以记录、保存并定期审查。	客户应确保系统管理员、操作员和用户的所有活动都记录、保存并定期审查。	华为云的**云审计服务（Cloud TraceService，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（Object Storage Service，简称OBS）**以实现日志的备份。 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。通过集中、完整的日志大数据分析系统，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。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

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			登录IP、登录方式及登录时间等。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。
3.1.8.4	系统跟踪记录应保留事件描述、事件源、事件时间、用户/系统信息、源地址、目标地址和交易详细信息，并应通过时间戳保护其完整性。	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。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。	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。 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。 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。
3.1.8.6	为了进行分析和审查，记录应收集在中央记录管理系统中，并由授权人员定期审查。当记录保存或发送过程中出现错误时，应启动并监控警告机制。	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，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 (Cloud Eye Service，简称CES)**，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。 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

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			对接。
3.1.8.8	应使用网络威胁与事件管理系统或记录分析工具，按照关联规则对网络事件进行检测和详细分析。	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 (Cloud Eye Service，简称CES)**，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。 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。

6.1.6虚拟化安全

编号	具体控制要求	客户关注点	华为云的应答
3.1.9.5	如果通过第三方提供虚拟化服务，则必须保证虚拟化环境的安全。	客户使用了第三方提供的虚拟化服务，必须保证虚拟化环境的安全。	华为内部的统一虚拟化平台（UVP - Unified Virtualization Platform）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。为保证平台安全，华为云对主机操作系统进行最小化裁剪并对服务做安全加固。同时，对接入主机操作系统的华为云管理员执行严格的权限访问控制 (PAM –Privilege Access Management)，对其所执行的各项运维运营操作实行全面的日志审计。华为云管理员必须经过双因子认证后，才能通过堡垒机接入管理平面，所有操作都会记录日志并及时传送到集中日志审计系统。 UVP 直接运行于物理服务器之上，提供虚拟化能力，为虚拟机提供运行环境。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			UVP 通过 CPU隔离、内存隔离和 I/O 隔离等技术手段实现虚拟主机操作系统与访客虚拟机操作系统之间的隔离，并通过 Hypervisor 让虚拟主机操作系统与访客虚拟机操作系统使用不同的权限运行，来保证平台系统资源的安全。更多关于华为云平台安全的信息请参见‘**华为云安全白皮书**’。

6.1.7 身份验证和访问管理

编号	具体控制要求	客户关注点	华为云的应答
3.1.12.2	应定义唯一标识其自身的用户帐户，并制定密码管理规则。	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**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。 华为云员工在内部办公网络中使用唯一身份标识，建立了完整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。 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，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，对认证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身份进行验证。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.12.3	应采取适当的安全措施（请求限制、IP 封锁、验证码等）来防止对登录机制的攻击，并记录不成功的登录尝试。	客户应采取适当的安全措施来防止对登录机制的攻击，并设定特定次数的登录失败尝试和登录日志记录，在登录失败后对账户进行锁定和调查。	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认证码进行二次认证。修改密码、手机等敏感信息时，**统一身份认证服务（Identity and Access Management，简称IAM）**默认启用多因子认证，并可支持密码规则配置，保证用户账号安全。 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，严格纳管回收特权账号。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，员工每次登录均需要使用多重身份验证确定身份。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录未遂事件进行报告。
3.1.12.5	系统管理员必须拥有单独的帐户才能执行需要提升权限（应该执行高权限操作）的操作。应为使用管理员帐户进行的交易创建审核记录。	客户应制定特权账号管理机制，控制和限制特权访问权限的分配和使用。	客户可使用华为云**统一身份认证服务（Identity and Access Management，简称IAM）**。IAM提供适合企业级组织结构的用户账号管理服务，为用户分配不同的资源及操作权限。华为云针对特权账号制定了管理要求，将特权账号分类，并在特权账号的创建、回收、授权、使用、注销等各阶段中遵守管理要求。 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。运维人员使用特权账号时需要提交工单申请，并例行开展相关审计，以确保特权账号的使用安全。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.12.6	非活动会话必须在一段时间后终止。	客户应制定安全会话管理，包括会话超时终止。	客户可使用**统一身份认证服务（Identity and Access Management，简称IAM）**，IAM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、密码更改周期、登陆策略、账号锁定策略、账号停用策略会话超时策略，提供基于 IP 的ACL。 华为云针对特权账号制定了管理要求，将特权账号分类，并在特权账号的创建、回收、授权、使用、注销等各阶段中遵守管理要求。 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。运维人员使用特权账号时需要提交工单申请，并例行开展相关审计，以确保特权账号的使用安全。
3.1.12.7	访问公司资源时应使用身份验证机制。	客户应制定访问公司资源时使用的身份验证机制。	客户可使用华为云**统一身份认证服务（Identity and Access Management，简称IAM）**，统一身份认证服务提供并默认启动多因子认证用以增强账号安全性。 华为云强调员工云服务账号的安全风险可控，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，员工每次登录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**虚拟专用网络（Virtual Private Network，简称VPN）**方可登录认证。
3.1.12.10	所有在一段时间内不使用且无法与业务流程或机构人员关联的帐户应自动禁用。	客户应确保在员工职位变更时对其相关权限进行审查和变更，并定期对内部账号/权限进行审查和清理。	华为云员工账号管理遵从公司用户账号权限管理规定。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。 同时，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。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.12.16	所有身份验证信息必须使用强加密算法存储并使用加密通道传输。	客户应确保身份验证信息使用强加密算法存储并使用加密通道传输。	客户可使用华为云提供的多种隐私保护技术及服务，包括**统一身份认证服务（Identity and Access Management，简称IAM）**、**密码安全中心（Data Encryption Workshop，简称DEW）**等，为客户提供身份验证信息的加密存储和加密传输。云使用 IAM 对访问进行管理，IAM对用户账号和密码等身份验证信息的存储和传输进行加密保护，以防止个人数据泄露，保证用户的个人数据安全。
3.1.12.18	应监控用户行为、用户角色和授权级别的变化，防止安全漏洞，并激活警报机制。	客户应根据制定的身份访问控制策略，对用户的访问控制进行管理，包括对用户行为、用户角色和授权级别的变化实施适当的监控，并制定预警处罚机制，在必要时触发警报。	华为云提供的**云审计服务（Cloud TraceService，简称CTS）**可以记录操作人员对华为云上的资源和系统配置的变更，供用户查询、审计和回溯使用。可实时、系统地记录所有人员的操作，以便客户对各项变更执行事后审计。华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，以确保支撑网络安全事件回溯。该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超过 180 天，90 天内可以实时查询。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。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，生成告警并通过应急响应值班人员进行分析处置，异常告警通过事件分析处理平台进行实时大屏监控与记录，同时华为云设置 7*24 的专业安全事件响应团队以及专家资源池，依照安全事件应急响应流程实时处理告警事件。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.12.19	应记录在存储/处理机密数据的系统上进行系统管理的会话期间进行的活动，并应验证收到的记录。	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。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。	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 (Cloud Eye Service，简称CES)**，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。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。 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。
3.1.12.21	当需要保证数据和密码的安全时，应使用自动密码管理工具（密码保险库）。	客户应考虑使用密码保险库保护、管理和存储密码。	客户可通过华为云**云堡垒机（Cloud Bastion Host，简称 CBH）**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。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。

版权所有 © 华为云计算技术有限公司

6.1.8 灾难恢复和业务连续性管理

编号	具体控制要求	客户关注点	华为云的应答
3.1.13.1	考虑到组织内业务流程中使用的所有系统和支持业务流程，应识别需要备份的系统，并应根据记录的备份计划进行备份管理。	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。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。	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（Cloud Backup and Recovery，简称CBR）**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（Elastic Volume Service，简称EVS）**中的快照功能，当数据丢失时，可通过快照将 数据完整的恢复到 快照时间点。华为云还为客户提供了**镜像服务（Image Management Service，简称IMS）**，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（Cloud Server Backup Service，简称CSBS）**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（Object Storage Service，简称OBS）**的版本控制、**云硬盘备份（Volume Backup Service，简称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。 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。同时，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。 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。单个区域内的不同可用区之间，通过高速光纤实现数据中心互联，满足跨可用区数据复制的基本要求，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

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			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通过后台自动修复，数据快速自动重建，使数据持久性可达 99.999999999%。 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，使系统设计数据持久性高达99.999999999999%。 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。
3.1.13.3	应创建备份交易的跟踪记录并使用时间戳保护	客户应创建备份交易的跟踪记录，同时考虑到信息安全要求和相关立法。	客户可使用华为云提供的**云日志服务（Log Tank Service，简称LTS）**，LTS 服务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。同时云日志服务可对系统组件的日志进行记录并保存，供客户进行日志审核。LTS云日志管理服务可结合**对象存储服务（Object Storage Service，简称OBS）**使用，对象存储服务中的多重安全防护如 SSL 传输加密、服务端加密、身份鉴权均可提供对所存储信息的安全保护。同时，传输数据时，OBS 支持 HTTPS/SSL 协议；如果您需要更高安全性，可以开启服务端加密功能。此外，OBS 控制台支持敏感操作保护，开启后执行删除桶等敏感操作时，系统会进行身份验证，进一步保证OBS 配置和数据的安全性。 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。同时，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

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			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。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。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。
3.1.13.4	为了确保系统、应用程序和数据的备份是可逆的，应定期进行回退测试，并为所执行的回退测试创建记录。	客户应定期对备份数据进行回退测试，以验证备份数据的可恢复性，并产生并保留测试记录。测试记录应包括测试的日期、测试的系统、测试是否成功、测试过程中遇到的问题等信息。	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。 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。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。同时，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 ISO 22301 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。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.13.5	应维护备份介质清单并定期审查清单。备份介质不应存放在与主要系统所在环境存在类似风险的其他环境中。应确认备份数据在从设施/场所传输时的安全性得到保证，并且环境的物理和逻辑安全得到保证。使用期限届满后，应按照国家/国际标准销毁备件，并保存销毁记录。	客户应明确关键技术和信息资产的备份范围，对关键业务数据、操作系统、应用软件进行备份。客户应确保已备份数据存放在安全的环境中，并且环境的物理和逻辑安全得到保证。使用期限届满后，应按照国家/国际标准安全销毁备件，并保存销毁记录。	客户可使用华为云存储容灾服务（SDRS - Storage Disaster Recovery Service）、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。 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。 同时，华为云制定并实施其内部办公移动介质管理规 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。 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。 除此之外，华为云对介质的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。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.13.9	作为业务连续性计划的一部分，还应考虑采购服务的连续性标准，以及提供服务的第三方的角色和责任。	客户应制定业务连续性计划灾难恢复计划，制定保证其关键业务连续的RTO、RPO 指标，并每年进行测试。客户应将第三方供应商的故障纳入响应和恢复计划，如果需要华为云协助执行客户的灾难恢复计划，华为云会积极配合。	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 ISO 22301 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。 华为云安全演练团队定期开展针对不同产品类型（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。当华为云的组织及环境发生重大变化时，也会对业务连续性的有效性进行测试。
3.1.13.14	作为灾难恢复计划的一部分，还应考虑第三方的角色和责任以及所提供服务的连续性。	客户应将第三方供应商的故障纳入响应和恢复计划，如果需要华为云协助执行客户的灾难恢复计划，华为云会积极配合。	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。 华为云安全演练团队定期开展针对不同产品类型（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。当华为云的组织及环境发生重大变化时，也会对业务连续性的有效性进行测试。
3.1.13.17	可能会增加“确保关键系统的连续性”。必须建立冗余结构，以确保机构认为至关重要的系统、服务、应用程序和基础设施的连续性。在部署业务时，需要进行冗余测试。应创建、衡量和报告服务水平协议。		

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.1.13.18	应建立灾难恢复中心，以便在发生灾难时维持信息系统功能。	客户应建立异地灾备中心，保障业务连续性。	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。 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 ISO 22301 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。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。 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。

 版权所有 © 华为云计算技术有限公司

6.2 应用程序和数据安全

6.2.1 数据库和记录管理

编号	具体控制要求	客户关注点	华为云的应答
3.2.7.13	应预先建立数据库管理系统备份和恢复机制，以防止数据误删除。应定期进行数据库备份。	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。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。	客户可以使用华为云提供的**云备份（Cloud Backup and Recovery，简称CBR）**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（Elastic Volume Service，简称EVS）**中的快照功能，当数据丢失时，可通过快照将数据完整的恢复到快照时间点。华为云还为客户提供了**镜像服务（Image Management Service，简称IMS）**，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（Cloud Server Backup Service，简称CSBS）**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（Object Storage Service，简称OBS）**的版本控制、**云硬盘备份（Volume Backup Service，简称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。 华为云建立了节点数据备份机制，通过 e-Backup 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。单个区域内的不同可用区之间，通过高速光纤实现数据中心互联，满足跨可用区数据复制的基本要求，用户可根据业务需求选择灾备复制服务。

版权所有 © 华为云计算技术有限公司

6.3 人员安全

6.3.1 一般安全措施

编号	具体控制要求	客户关注点	华为云的应答
3.5.1.4	在向人员和承包商提供对机构资产的访问权限之 前，应在与人员和承包商签订的合同中明确信息安全责任。	客户应在外包协议中明确其与服务提供商各自的信息安全职责。	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制化。华为云内部也建立了完善的供应商管理机制，会对外包商以及外包人员进行严格的安全管理，并会定期对供应商进行审计和安全评估。华为云会将客户在合同中的安全要求传递给供应商，确保供应商提供的产品和服务能满足华为云客户的安全要求。此外华为云会根据不同客户的需求，在重要供应商发生变更时，及时对客户进行通知。 同时，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。

6.3.2 供应商关系安全

编号	具体控制要求	客户关注点	华为云的应答
3.5.3.3	信息安全要求应添加到与每个可以访问、操作、存储、传输或提供组织资产的 IT 基础设施组件的供应商签订的合同中。	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。	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。

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.5.3.7	应与承包商的合同中明确规定如何处理承包商提供的服务和产品供应范围发生变化的情况。	客户应在合同中规定承包商提供的服务和产品供应范围发生变化的情况。	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制化。客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。
3.5.3.8	如果主承包商使用分包商来交付所提供的产品和服务；主承包商和分包商的角色和责任应记录在案，并且应从主承包商处获得分包商将在整个采购过程中遵守信息安全要求的承诺。	客户应对服务提供商的分包安排进行监控，与服务提供商在外包协议中约定分包的规则和限制，确保分包安排不会影响服务提供商对外包协议的履行，并且应从主承包商处获得分包商将在整个采购过程中遵守信息安全要求的承诺。	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制化。华为云内部也建立了完善的供应商管理机制，会对外包商以及外包人员进行严格的安全管理，并会定期对供应商进行审计和安全评估。华为云会将客户在合同中的安全要求传递给供应商，确保供应商提供的产品和服务能满足华为云客户的安全要求。此外华为云会根据不同客户的需求，在重要供应商发生变更时，及时对客户进行通知。同时，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。
3.5.3.9	为了确保满足信息安全要求，应定期审查和记录供应商服务。	客户应根据计划的频率定期审查和更新与第三方签订的网络安全协议与条款。	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。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。

版权所有 © 华为云计算技术有限公司

6.4 物理场所的安全

6.4.1 系统机房/数据中心的安全措施

编号	具体控制要求	客户关注点	华为云的应答
3.6.2.5	在系统机房/数据中心，应定期使用水、电、湿度、温度和烟雾控制系统。应确定这些系统想·的正常值和阈值，并建立报警机制，在超过预设阈值时，向有关人员发布告警。不应在室外安装环境监测系统用于远程监测和检查。	客户应关注云服务提供商数据中心的物理和环境安全。	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。华为云数据中心会考虑在政治稳定、社会犯罪率低、地理环境友好的地区选 址，远离洪水、飓风、地震等自然灾害隐患区域，避开强电磁场干扰，并对于周围的隐患区域设定了最小距离的技术要求。 同时，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。华为云数据中心建筑防火等级均按一级设计施工，使用了 A 级防火材料，满足国家消防规范。采用了阻燃、耐火电缆，在管内或线槽铺设，并设置了漏电检测装置。部署了自动报警和自动灭火系统，能够迅速准确发现并通报火情。自动报警系统与供电、监控、通风设备联动，即使意外情况造成无人值守，也能开启自动灭火系统得以控制火情。 除此之外，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。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。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
3.6.2.7	系统机房/数据中心的电线源、UPS 及发电机的燃油箱必须是冗余的，并必须定期对UPS、发电机燃油箱进行维护、测量和测试以及记录。 专家应按照制造商建议的时间间隔定期维护系统机房/数据中心服务设施以及进行接地测量，并应记录所有相关操作和结果	客户应确保云服务提供商采取适当措施，以解决电源故障和中断问题。	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。在机房供电线路上配置了稳压器和过压防护设备。在供电设备及线路上还设置冗余或并行的电力电缆线路为计算机系统供电。
3.6.2.8	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）。	客户应确保云服务提供商记录和实施物理安全保护措 施，防止数据中心物理和环境危害。	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。数据中心不但有妥善的选址，在设计施工和运营时，合理划分了机房物理区 域，合理布置了信息系统的组件，以防范物理和环境潜在危险（如火灾、电磁泄露等）和非授权访问。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。例如，华为云数据中心机房铺设了防静电地板，导线连接地板支架与接地网，机器接地以导走静电。在机房大楼顶部设置了避雷带，供电线路安装了多级避雷 器，导走电流。并且，华为云数据中心机房选址一定程度上决定面临的自然灾害以及可能的环境威胁。华为云数据中心选址一律避开自然灾害不利或危险的地区，减少周边环境对数据中心产生的干扰，如 400 米内无实验室、化工厂等危险区域。

版权所有 © 华为云计算技术有限公司

6.5 个人数据的安全

6.5.1 记录管理

编号	具体控制要求	客户关注点	华为云的应答
4.1.1.2	个人数据存储和销毁政策应根据《个人数据删除、销毁或匿名化规定》制定，并考虑机构编制的个人数据处理清单。	客户应依据《个人数据删除、销毁或匿名化规定》管理要求，制定个人数据留存规范，并确定个人数据处理清单和保留期限。	华为云处理的个人数据主要包括账号数据和客户数据。 （1）华为云作为账号数据的控制者在客户与华为云互动过程中，客户向华为云提交的账号数据，华为云决定了账号数据收集方式及处理目的，因此华为云承担数据控制者角色。华为云也将基于土耳其隐私法律的要求负责该部分客户个人数据的安全及隐私保护，确保个人数据的收集、处理、存储、传输过程符合法律规定，响应个人数据主体权利请求。 （2）华为云作为客户数据的处理者 客户拥有并完全控制客户数据，客户选择以及使用华为云服务存储和处理客户数据，客户通过云服务提供的功能配置或 API 接口等方式下达指示，华为云按照客户下达的指示处理数据，当客户是客户数据控制者角色时，华为云承担客户数据处理者角色。当客户是客户数据处理者角色时，华为云承担客户数据子处理者角色。详情请见《土耳其网络安全与隐私保护遵从性说明》 7.2-7.3 章。

 版权所有 © 华为云计算技术有限公司

6.5.2 个人数据管理流程的运作

编号	具体控制要求	客户关注点	华为云的应答
4.1.8.5	当个人信息被他人非法获取、公开、披露或者泄露时，应通过适当的方式（网页、电子邮件、短信等）告知相关人员和依法需要通报的机构、组织。	客户应制定数据泄露通报机制，当发生数据泄露时间 时，通过适当的方式告知相关人员和依法需要通报的机构、组织。	客户可选择华为云安全云脑实现智能高效的威胁检测与响应处置。安全云脑可通过每天对数万亿安全日志进行分析，利用华为云安全运营团队多年沉淀经验、内置机器思维降低合法事件的干扰，帮助客户从海量的安全日志中发现威胁。 为配合客户满足合规要求，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。除此之外，华为云已建立了数据泄露事件处理机制，如有必要，华为云会按照适用法律法规的要求进行事件通 报。如客户需进行监管上报的工作，华为云将配合客户提供相关材料。

 版权所有 © 华为云计算技术有限公司

6.6 云计算安全

6.6.1 一般安全措施

编号	具体控制要求	客户关注点	华为云的应答
4.3.1.2	在云计算服务范围内，服务提供者与服务接收机构应当签订合同，其中包括相互义务和保密条款。合同中应充分规定所接受的服务范围，并应根据服务范围内处理的数据的重要性采取适当的安全措施，应确定相关合同的有效期并定期审查。	客户与其云服务供应商签订的合同中应清楚列明网络安全责任和义务，以及服务供应商在合约下的所提供的服务内容和水平，包括采取适当的安全措施等。 客户应定期审查和更新与服务提供商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。此外，其中还包括了华为云所实施的安全措施。例如，加密、访问控制、事件管理、配置管理、对。华为云将持续更新和完善安全措施，确保客户数据的安全性。 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。并且，华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户对华为云的审计和监督。
4.3.1.3	云计算下运行的所有系统之间的数据通信必须使用安全且最新的通信协议进行，并且当数据传输到云环境时，必须确保数据传输为单向且企业网络与云环境隔离。	客户应使用最新的网络安全传输协议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（Virtual Private Network，简称 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。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 **虚拟私有云（Virtual Private Cloud，简称 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 IP Sec VPN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：REST 网络通道是将服务以标 RESTful 的形式向外发布，调用端直接使用 HTTP 客户端，通过标准 RESTful 形式对 API 进行调用，实现数据传输；Highway 通道是高性能私有协议通道，在有特殊性能需求场景时可选 用。上述两

版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			种数据传输方式均支持使用传输层安全协议（TLS –Transport Layer Security）1.2 及以上版本进行加密传输，同时也支持基于X.509证书的目标网站身份认证。
4.3.1.4	使用相同云的组织应该在网络层面上彼此逻辑和/或物理隔离。	客户应确保其使用的云环境与其他组织系统使用相同云环境在网络层面上相互逻辑和/或物理隔离。	客户可选择华为云，华为云提供的**虚拟私有云（Virtual Private Cloud，简称VPC）**）服务，实现不同区域之间网络隔离。VPC 可为租户构建出私有网络环境，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络 ACL 和安全组规则，对进出子网和虚拟机的网络流量进行严格的管控，满足租户更细粒度的网络隔离需求。华为云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。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
4.3.1.5	在云服务范围内，如果有需要，服务提供商应允许不可逆转地删除用作模板的镜像。	客户应在云服务提供商签订的合同协议中明确云服务提供商服务范围和安全责任，包括实施适当的安全措施确保镜像安全管理。	客户可选择华为云**镜像服务（Image Management Service，简称IMS）**提供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。 用户可以直接使用公共镜像，或者通过已有的云服务器或使用外部镜像文件自行创建私有镜像，也可以参与创建和维护共享镜像。并且，华为云支持对虚拟机镜像文件进行完整性、机密性保护，并确保虚拟机的镜像、快照的剩余信息得到完全清除。华为云为客户提供自主可控的数据删除机制，当前为客户提供的数据删除机制主要涵盖以下场景： 针对存储及数据库等云服务，客户可在服务层面自行执行数据删除操作。 华为云建议客户对云上重要数据进行加密存储，当加密数据需要删除时，通过直接删除相关数据加密密钥从而删除数据，防止数据在被彻底删除前被恢复为明文后造成泄露。 在客户的云服务资源到期未续订或欠费的场景下，华为云仍然可提供自主可控的数据删除机制。当客户的云服务资源到期未续订或欠费时，华为云将向客户提供宽限期，宽限期内客户可正常访问及使用云服务。宽限期到期后客户仍未续订或未缴清欠款时，云服务将进入保留期。保留期内客户不能访问云服务，但对客户存储在云服务中的数据仍予以保留。当保留期到期后客户仍未续订或充值，华为云才将删除客户存储在云服务中的所有数据，给予客户充分的时间，自行决策删除与保留数据。 用户提交注销账户请求时，账户下的所有数据也将被删除。在以上数据删除场景，华为云将在平台层面将对待删除的数据及其副本进行全面的清除。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
4.3.1.6	当云服务范围内的任何虚拟机终止服务时，服务提供商应自动删除该虚拟机在云计算服务器中的内存区域且不可逆。	客户应在与第三方签订的合同或协议中明确云服务提供商的服务范围和安全责任，包括当服务协议终止时，云服务提供商应自动删除虚拟机在云计算服务器中的内存区域且不可逆。	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。在物理介质销毁层面，为保证数据中心介质生命周期末期数据安全，华为云参照相关行业标准，实施了完善的存储介质处置机制。如参考 NIST SP 800-88标准对存储介质进行处理，针对需要重复使用的存储介质，进行随机数覆写、加密擦除等方式进行数据安全删除，针对不需要重复使用的存储介质则采取消磁、物理损毁等方式进行物理销毁。
4.3.1.7	服务提供商必须能够保护自己的资源免受 DDoS 攻击的影响，并确保业务和服务的连续性，以抵御超出其能力范围的大规模 DDoS攻击。在与服务接收方签订的合同和承诺中，应包含此方面。 此外，服务提供商应采取防火墙和入侵检测系统等安全措施，以防止其他服务区域受到网络攻击（退役、恶意软件等）的影响或该攻击可能导致系统性能问题。 服务提供商还应确定、衡量和报告与服务提供商提供的服务相关的服务水平承诺条件。机构应寻求云服务提供商提供的服务，这些服务提供商实施适合资产组重要性的安全措 施，并定期进行安全审计。 运营商应采取措施，在访问服务器时将流量保持在国内。在使用云服务时，属于机构的加密密钥应由接受服务的机构管理。应使用 IPSec 或 SSL VPN网关通过云管理界面进行操作，并且只能通过这些通道访问云管理界面。	客户应选择在土耳其部署服务器的云服务提供商，确保在访问服务器时将流量保持在国内，并且云服务提供商应部署防火墙和入侵检测系统、使用安全通道访问云管理界面（如 IPSec或 SSL VPN 网关）、实施适当的安全措施以及定期执行安全审计。此外，客户应在与第三方签订的合同或协议中明确云服务提供商的服务水平协议和安全责任，包括确保业务和服务的连续性，以防御大规模 DDoS 攻击等。	华为云土耳其等全球多个区域提供云服务。客户可以选择上述任意区域的云服务来存储和处理客户数据。 华为云遵循 ISO 27001、 ISO 20000、ISO 22301 等国际标准建立完善的信息安全管理体系、IT服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题，并实施整改，推动管理体系的持续改进。实现高可靠、智能化的云安全防护和自动化的云安全运维运营体系。 3. 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）。华为云运维管理区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。 除了上述网络分区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，对认证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身份进行验证。

 版权所有 © 华为云计算技术有限公司

编号	具体控制要求	客户关注点	华为云的应答
			华为云为客户提供了多种类型的数据库服务，数据库服务内置了内置多种安全特性来保障租户数据库的可靠性和安全性，例如 **虚拟私有云（Virtual Private Cloud，简称 VPC）**、安全组、权限设置、SSL 连接、自动备份、数据库快照、时间点恢复（PITR – Point In Time Recovery）、跨可用区部署等。华为云数据库服务支持用户自定义数据库账户密码策略。用户可自行修改密码复杂度、密码有效期、密码重用设 置、加密方式和锁定方式的配置。
5.2.1.5	应尽可能限制与数据库服务器的远程连接，并将其配置为仅允许授权用户和/或应用程序进行远程访 问。在这种情况下，应对服务器进行安全配置，并在网络层采取必要的措施。	客户应对数据库访问制定访问控制措施，仅允许授权用户或应用程序远程访问数据库。	华为云为客户提供了多种类型的数据库服务，数据库服务内置了内置多种安全特性来保障租户数据库的可靠性和安全性，例如 **虚拟私有云（Virtual Private Cloud，简称 VPC）**、安全组、权限设置、SSL 连接、自动备份、数据库快照、时间点恢复（PITR – Point In Time Recovery）、跨可用区部署等，详情请参见《华为云安全白皮书》。

 版权所有 © 华为云计算技术有限公司

7 华为云为客户提供的安全与隐私保护相关的云服务

客户负责客户数据安全，为保障客户内容安全，客户可以根据客户内容适合的安全级别，采取额外的安全措施，额外的安全措施可以来源华为云，也可来源第三方。

华为云理解客户的安全与隐私保护需求，并结合自身丰富安全与隐私保护实践及技术能力，提供了相关的安全与隐私保护相关云服务供客户选择。云服务涵盖网络、数据库、安全、管理与部署工具等产品，相关产品的数据保护、数据删除、网络隔离、权限管理、容灾备份、安全审计等功能可帮助客户加强安全保障。

- **安全合规**

产品名称	产品介绍	核心功能
Web 应用防火墙 Web Application Firewall (WAF)	WAF可对网站业务流量进行多维度检测和防护，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，阻挡诸如SQL注入或跨站脚本等常见攻击。 客户可使用WAF保护其网站或服务器免受外部攻击，避免这些攻击影响Web应用程序的可用性、安全性或过度消耗资源，降低数据被篡改、失窃的风险。	安全防护
云防火墙 Cloud Firewall (CFW)	CFW是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持按需弹性扩容、AI提升智能防御能力、灵活扩展满足云上业务的变化和扩张需求，让用户快速灵活应对威胁。 云防火墙服务是为用户业务上云提供网络安全防护的基础服务。	资产保护 访问控制 在线防御
企业主机安全 Host Security Service (HSS)	HSS能提供资产管理、漏洞管理、基线检查、入侵检测等功能，能够帮助企业更方便地管理主机安全风险，实时发现并阻止黑客入侵行为。 客户可通过HSS更方便地管理主机、容器的安全风险，实时发现勒索、挖矿、渗透、逃逸等入侵	资产管理 漏洞管理 入侵检测

 版权所有 © 华为云计算技术有限公司

产品名称	产品介绍	核心功能
	行为，以满足等保合规的要求。	
数据库安全服务 Database Security Service (DBSS)	DBSS 是一款智能的数据库安全服务，基于机器学习机制和大数据分析技术，提供数据库审计，SQL 注入攻击检测，风险操作识别等功能。 客户可通过DBSS检测潜在风险，保障云上数据库的安全。	安全审计
密码安全中心 Data Encryption Workshop (DEW)	DEW 是一款综合的云上数据加密服务，提供专属加密、密钥管理、密钥对管理等功能。其密钥由硬件安全模块保护，并与华为云其他服务集成。客户也可以借此服务开发自己的加密应用。 客户可采用DEW进行密钥全生命周期集中管理，保障数据存储过程中的完整性。	数据加密
DDoS防护 Anti-DDoS Service (AAD)	AAD 是一款保护互联网服务器免受大流量 DDoS 攻而击导致不可用的增值服务。 客户可以通过AAD产品配置高防IP，将攻击流量引流到高防IP清洗，确保源站业务稳定可靠。	安全防护
数据安全中心 Data Security Center (DSC)	DSC 是新一代的云原生数据安全平台，提供数据分类分级，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。 客户可通过DSC整合数据安全生命周期各阶段状态，构建云服务全景图，保护数据采集、存储/传输、使用、交换/销毁的安全。	数据分级分类 数据脱敏 数据水印
云堡垒机 Cloud Bastion Host (CBH)	CBH 是华为云的一款 4A 统一安全管控平台，为企业提供集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体的运维管理服务。 客户可通过CBH对云主机进行远程运维，提高客户的访问控制安全能力，保护资源运维和系统管理的安全性，降低系统和运维资源被非法入侵的风险。	权限管理
云证书与管理服务 Cloud Certificate Manager (CCM)	CMM 是一个为云上海量证书颁发和全生命周期管理的服务，提供 SSL 证书管理和私有证书 管理服务。 客户可通过CCM提高对SSL证书和私有证书的 保密性和安全性，提升访问和传输通道的安 全，降低数据在传输和访问过程中被非法入	证书管理
安全云脑 SecMaster	安全云脑基于云原生安全，提供全面的日志采集、安全治理、智能分析、态势感知、编排响应等快速闭环的安全信息和事件管理能力，实现自动化安全运营，助客户守护云上安全。	态势感知 安全运营

 版权所有 © 华为云计算技术有限公司

- **存储**

产品名称	产品介绍	核心功能
云备份 Cloud Backup and Recovery (CBR)	CBR为云上的弹性云服务器、裸金属服务器、云硬盘、云下VMware虚拟化环境和本地文件 目录，提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数据恢复到任意备份点。	数据备份
云硬盘备份 Volume Backup Service (VBS)	VBS 为云硬盘创建在线永久增量备份，并对加密盘发备份数据自动加密，并可将数据恢复到任意备份点，增强数据可用性。 VBS可降低病毒入侵、人为误删除、软硬件故障等事件的发生的可能性，保护数据安全可靠，降低数据被非法篡改的风险。	数据备份
云服务器备份 Cloud Server Backup Service (CSBS)	CSBS 可同时为云服务器下多个云硬盘创建一致性在线备份。 CSBS可降低病毒入侵、人为误删除、软硬件故障等事件的发生的可能性，保护数据安全可靠，降低数据被非法篡改的风险。	数据备份

- **管理与监督**

产品名称	产品介绍	核心功能
统一身份认证服务 Identity and Access Management (IAM)	提供身份认证和权限管理功能，可以管理用户（比如员工、系统或应用程序）账号，并且可以控制这些用户对其名下资源的操作权限。 客户可通过IAM采取适合的用户管理、身份认证和细粒度的云上资源访问控制等措施，防止对内容数据进行的未授权修改。	权限管理
云审计服务 Cloud Trace Service (CTS)	为客户提供云账户下资源的操作记录，实现安全分析、合规审计、问题定位等场景。 客户可以通过配置CTS对象存储服务，将操作记录实时同步保存至CTS，以便保存更长时间的操作记录，保障数据主体的知情权、实现快速查找。	安全审计
云监控服务 Cloud Eye Service (CES)	为客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。 客户可通过CES全面了解华为云上的资源使用情况、业务的运行状况，并及时收到 异常报警做出反应，保证业务顺畅运行。	安全审计
云日志服务 Log Tank Service (LTS)	提供日志收集、实时查询、存储等功能，无需开发即可利用日志做实时决策分析，提升日志处理效率，帮助用户轻松应对日志实时采集、查询分析等日常运营、运维场景。 客户可通过LTS保留对个人信息的操作记录，保障数据主体的知情权。	安全审计

 版权所有 © 华为云计算技术有限公司

产品名称	产品介绍	核心功能
配置审计 Config	配置审计（Config）服务提供全局资源配置的检索，配置历史追溯，以及基于资源配置的持续的审计评估能力。 客户可通过Config查看资源详情、资源之间的关系、资源历史，并可以通过配置合规规则来对资源进行合规性检查，确保云上资源配置变更符合预期。	安全审计

- **网络**

产品名称	产品介绍	核心功能
虚拟专用网络 Virtual Private Network (VPN)	VPN 用于搭建客户本地数据中心与华为云 VPC 之间便捷、灵活，即开即用的 IPsec 加密连接通道。 客户可通过VPN实现灵活一体，可伸缩的混合云计算环境，并且由于VPN的加密特性，提高了客户的安全	安全传输
虚拟私有云 Virtual Private Cloud (VPC)	VPC 是客户在华为云上的隔离的、私密的虚拟网络环境。客户可以自由配置 VPC 内的 IP 地址段、子网、安全组等子服务，也可以申请弹性带宽和弹性 IP 搭建业务系统。 VPC是客户的云上私有网络，各客户之间100%隔离，增强云上数据的安全性。	网络隔离

 版权所有 © 华为云计算技术有限公司

8 结语

华为云致力于为土耳其云用户提供符合监管要求的安全的云环境，并持续运营华为云安全保障体系。本文描述了华为云在监管重点领域下的安全实践，有助于土耳其云用户详细了解华为云网络安全方面的遵从性，让客户安全、放心地使用华为云。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合土耳其监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

本白皮书仅供参考，不具备任何法律效力或构成任何形式的法律建议。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监管要求的遵从性。

 版权所有 © 华为云计算技术有限公司

9 版本历史

日期	版本	描述
2026 年 7 月	1.0	首次发布

 版权所有 © 华为云计算技术有限公司