华为云泰国云安全遵从性指南

文档版本 1.0

发布日期 2026-05-11

华为云计算技术有限公司

商标声明

和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为云计算技术有限公司

地址: 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址: **https://www.huaweicloud.com/**

目 录

1 概述

1.1 背景与发布目的

信息科技的迅猛发展，越来越多的组织在逐渐寻求业务转型并希望借助先进的技术以降低成本、提升运营效率、实现业务模式的创新。为了规范对于信息科技的运用，泰国国家网络安全委员会发布了一系列监管要求、指南和通知，针对泰国云服务管理、应用、实施等方面提出了相关细节要求。

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泰国网络安全监管要求，详细阐述华为云将如何协助其满足这些监管要求。

1.2 适用的网络安全监管要求简介

泰国国家网络安全委员会(National Cyber Security Committee, NCSC)是泰国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。国家网络安全办公室 (Office of the National Cyber Security Agency, NCSA)作为 NCSC 的常设执行与操作机构，负责具体的监管落地。这包括发布细化的安全准则、执行合规审计、管理网络安全事件通报流程，以及与国际组织及云服务商(CSP)进行技术对接。

- **《网络安全法 B.E. 2562 (2019)》 (Cybersecurity Act)**：泰国国民议会于 2019 年 2 月 28 日正式通过，并于 2019 年 5 月 27 日起正式施行。该法案建立了泰国国家网络安全监督与维护的法律框架。该法案要求或授权采取措施预防、管理和应对网络安全威胁和事件，并规范了关键信息基础设施 (CII) 的所有者或运营者、政府机构、关键基础设施相关实体，以及与之相关的事项。本法规云计算场景相关要求在《云安全标准》中细化，本指南不开展详细解析。
- **《云安全标准》 (Cybersecurity Standards for Cloud Systems)**：泰国网络安全委员会 2024 年 5 月发布了《泰国云安全标准》。该规定从云安全治理、信息安全政策、信息安全组织、合规性、云基础设施与运营、人力资源安全、资产管理、访问控制、密码学、物理与环境安全等领域提出对云安全管理相关要求。

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。

- **云计算**

  是指通过自助服务配置和按需管理来访问由可共享、可扩展且可伸缩的物理或虚拟资源组成的信息网络的概念。

- **云服务**

  指的是执行云计算的能力，可通过指定接口进行访问。

- **云服务类别**

  是指一组具有某些共同特征的云服务，主要分类如下：

  基础设施即服务(IaaS)：由计算系统、数据存储、网络和其他相关资源组成，用户可以在所提供的基础设施上高效使用软件，而无需管理底层基础设施。

  平台即服务(PaaS)：包括应用平台、数据库和计算机服务，用户可以在此环境中开发、部署和配置软件，而无需管理底层基础设施。

  软件即服务(SaaS)：提供商提供即用型软件，并且用户管理配置、参数、处理单元和存储，以实现其服务目标。

- **公共云**

  是指任何云服务用户均可访问的云服务，其资源由云服务提供商控制。

- **云服务客户(Cloud Service Customer，CSC)**

  是指与云服务提供商签订正式合同，使用其提供的云服务的机构。

- **云服务提供商(Cloud Service Provider, CSP)**

  是指向客户提供云服务的公共或私人实体，负责管理资源以确保其用户的可用性、安全性和可扩展性。

  。

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ISO9001基础上的，由全球电信业优

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ISO9001的所有要求，ISO9001将来的任何改动也会导致TL9000的改动。 华为云取得了ISO9001 / 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	BS10012是BSI发布的个人信息数据管理体系标准，BS10012认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。
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

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。

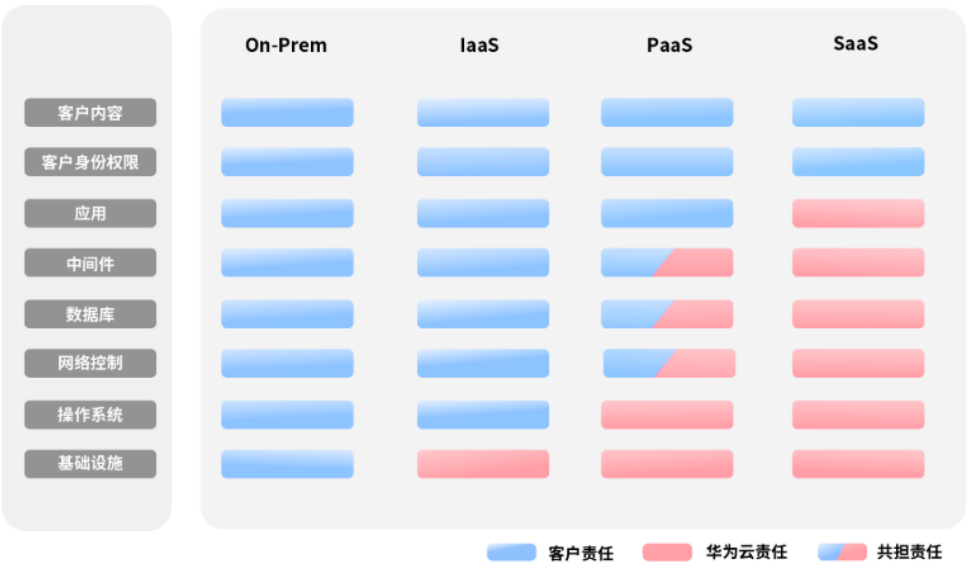
3 华为云责任共担模型

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 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。

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 泰国 Region 和可用区(AZ)示例

5 华为云如何遵从及协助客户满足《泰国云安全标准》的要求

泰国国家网络安全委员会(NCSC)于 2024 年 5 月发布了《泰国云安全标准》。该规定从云安全治理、信息安全政策、信息安全组织、合规性、云基础设施与运营、人力资源安全、资产管理、访问控制、密码学、物理与环境安全等领域提出对云安全管理相关要求。

客户在遵循《泰国云安全标准》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《泰国云安全标准》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助客户满足这些控制要求。

5.1 云安全治理

5.1.1 信息安全政策

编号	具体控制要求	客户关注点	华为云的应答
5.1.1 信息安全政策	**云服务客户** a) 云服务客户应将云计算信息安全策略定义为针对特定主题的策略。云服务客户针对云计算的信息安全策略应与其组织对信息及其他资产可接受的信息安全风险水平保持一致。 b) 在制定云计算信息安全策略时，云服务客户应考虑以下因素： - 存储在云计算环境中的信息可能受到云服务提供商的访问和管理； - 资产可能保留在云计算环境中，例如应用程序；	1. 客户应制定云安全策略，策略需考虑CSP对云上信息的访问和管理、拥有特权的管理员、CSP的位置及客户数据存储的位置等因素； 2. 隐私政策应声明遵守个人数据保护法规、CSC与CSP之间的合同； 3. CSC与CSP之间的合同应清晰划分双方责任。	1. 为配合客户遵从监管要求，华为云不仅明确定义了与客户之间的安全责任共担模型，也提供了线上的《华为云用户协议》以及华为云《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。 2. 华为云作为服务提供商，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

编号	具体控制要求	客户关注点	华为云的应答
	- 流程可能在多租户、虚拟化的云服务上运行； - 使用云服务的云服务用户及其使用云服务的场景； - 拥有特权访问权限的云服务客户的云服务管理员； - 云服务提供商所在组织的地理位置，以及云服务提供商存储云服务客户数据(即使为临时存储)的国家。 c) 个人数据保护政策应增加一项声明，表明支持并承诺遵守适用的个人数据保护法律法规，以及云服务提供商与云服务客户之间约定的合同条款。 d) 合同协议应明确划分云服务提供商、其分包商与云服务客户之间的责任，同时考虑所涉云服务的类型(例如云计算参考架构中的IaaS、PaaS或SaaS类服务)。例如，应用层控制措施的责任划分可能因云服务提供商提供的是SaaS服务，还是提供云服务客户在其上构建或部署自身应用程序的PaaS或IaaS服务而有所不同。 **云服务提供商** a) 云服务提供商应扩展其信息安全策略，以涵盖云服务的提供和使用，并考虑以下因素： - 适用于云服务设计和实施的基本信息安全要求； - 来自授权内部人员的风险； - 多租户及云服务客户之间的隔离(包括虚拟化)； - 云服务提供商员工对云服务客户资产的访问；		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。

编号	具体控制要求	客户关注点	华为云的应答
	- 访问控制程序，例如对云服务管理访问实施强身份验证； - 变更管理过程中与云服务客户的沟通； - 虚拟化安全； - 对云服务客户数据的访问及保护； - 云服务客户账户的生命周期管理； - 通报安全事件以及信息共享指南，以支持调查和取证工作。		

5.1.2 信息安全组织

编号	具体控制要求	客户关注点	华为云的应答
5.1.2.1 信息安全角色和责任	**云服务客户** a) 云服务客户应与云服务提供商就信息安全角色和责任的适当分配达成一致，并确认其能够履行所分配的角色和责任。双方的信息安全角色和责任应在协议中明确说明。 b) 云服务客户应识别并管理其与云服务提供商客户支持与服务职能之间的关系。 **云服务提供商** a) 云服务提供商应与云服务客户、其自身的云服务提供商及供应商就信息安全职责的适当分配达成一致，并形成书面记录。 b) 云服务提供商应指定一名数据保护官，作为与云服务客户的联络人。	1. 客户应明确与云服务提供商双方的信息安全角色和责任，并在协议中明确说明。 2. 客户需主动管理其与提供商支持团队的关系，确保沟通与协作顺畅。	华为云作为云服务提供商： 1. 华为云不仅明确定义了与客户之间的安全责任共担模型，也提供了线上的**《华为云用户协议》**以及华为云**《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，华为云制定了线下合同模板，可根据不同客户的需求进行定制化。 2. 华为云根据法律要求，设立了数据保护官。如有任何问题、意见或建议等，客户可以通过**dposg@huaweicloud.com**与数据保护官联系。
5.1.2.2 沟通和授权	**云服务客户** a) 云服务客户应确定与云服务客户和云服务提供商联合运营相关的主管部门。	客户应确定与云服务客户和云服务提供商联合运营相关的主管部门。	1. 华为云提供了线上的**《华为云用户协议》**以及**《隐私政策声明》**，其中告知华为云所在的地理区域。 2. 华为云以区域(Region)为单位向客户提供服务。区域即客户

编号	具体控制要求	客户关注点	华为云的应答
	云服务提供商 a) 云服务提供商应向云服务客户告知其组织所在的地理区域，以及云服务客户数据可能被存储的国家。		内容数据的存储位置，华为云绝不会在未经用户授权的情况下，跨区域移动客户的内容数据。客户在使用云服务时，建议根据就近接入原则并遵从不同地域的法律法规要求选择区域，确保其内容数据存储在目标位置。对于区域服务，客户可以在购买服务初期按需选择区域，其服务部署位置及数据留存地可以通过华为云门户进行变更。

5.1.3 合规性

编号	具体控制要求	客户关注点	华为云的应答
5.1.3.1 识别适用法规和合同要求	**云服务客户** a) 云服务客户应考虑到，相关法律法规可能不仅包括约束云服务客户的司法管辖区的法律法规，还可能包括约束云服务提供商的司法管辖区的法律法规。 b) 云服务客户应要求云服务提供商提供其符合云服务客户业务所需相关法规和标准的证明。此类证明可由第三方审计机构出具的认证文件提供。 **云服务提供商** a) 云服务提供商应向云服务客户告知管辖该云服务的法律管辖区。 b) 云服务提供商应明确其自身相关的法律要求(例如，关于加密以保护个人数据的要求)。该信息应在客户请求时提供给云服务客户。 c) 云服务提供商应向云服务客户提供其当前符合相关法律法规及合同要求的证明文件。	1. 客户需主动识别并遵守自身及提供商所在司法管辖区的法律法规，并应要求提供商提供符合业务所需法规的第三方审计证明。同时，提供商负有明确的告知义务，必须向客户说明管辖服务的法律管辖区，并在客户请求时明确其自身的法律要求。 2. 要求云服务提供商提供其符合云服务客户业务所需相关法规和标准的证明。	1. 华为云提供了线上的**《华为云用户协议》**，其中明确告知客户法律管辖区。 2. 华为云始终遵守泰国云服务相关的法律法规要求，并且华为云已通过 ISO 27001、SOC、ISO 27017、ISO 27018、CSA STAR等多项国际安全与隐私保护认证，并每年接受第三方审计。如有必要，客户可以通过官方渠道向华为云申请获取证书以及审计报告的副本。 3. 华为云也严格遵守泰国个人数据保护法PDPA的要求，详情见**华为云泰国PDPA遵从性指南**。
5.1.3.2	**云服务客户** a) 在云服务中安装商业许可	客户在允许任何许可软件安装到云服务之前，	华为云提供在线版本的**《华为云服务等级协议》**，明确了提供的服务

编号	具体控制要求	客户关注点	华为云的应答
知识产权	软件可能导致违反该软件的许可条款。云服务客户应在允许任何许可软件安装到云服务之前，制定相应流程以识别与云环境相关的特定许可要求。尤其应注意云服务具有弹性与可扩展性的情况，防止软件运行的系统数量或处理器核心数超出许可条款允许的范围。 **云服务提供商** a) 云服务提供商应建立处理知识产权投诉的流程。	制定相应流程以识别与云环境相关的特定许可要求。	的内容和级别，以及华为云的职责。华为云将派专人积极配合客户的知识产权投诉相关事宜。
5.1.3.3 记 录保护	**云服务客户** a) 云服务客户应向云服务提供商请求有关由云服务提供商收集和存储的、与云服务客户使用云服务相关的记录保护情况的信息。 **云服务提供商** a) 云服务提供商应向云服务客户披露其收集和存储的、与云服务客户使用云服务相关的记录保护信息。	客户应向云服务提供商请求有关由云服务提供商收集和存储的、与云服务客户使用云服务相关的记录保护情况的信息。	1. 为协助客户满足监管要求，华为云的**云审计服务(Cloud Trace Service，简称CTS)**可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。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，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 2. 作为云服务提供商，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，并遵守各国《个人数据保护法》所述的数据保护原则。
5.1.3.4 加密控制措施	**云服务客户** a) 云服务客户应验证适用于云服务使用的加密控制措施集合是否符合相关协议、法律法规。 **云服务提供商** a) 云服务提供商应向云服务	客户需主动验证云服务中使用的加密控制措施是否符合相关协议和法律法规的要求。	1. 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。针对于加密，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

编号	具体控制要求	客户关注点	华为云的应答
	客户提供其所实施的密码控制措施的说明，以供客户审查其是否符合相关协议、法律法规的要求。		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**虚拟专用网络(Virtual Private Network，简称VPN)**和应用层 TLS 与证书管理，华为云服务为客户提供控制台和 API 两种访问方式，均采用加密传输协议构建安全的传输通道。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。针对于静态数据，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。首先，华为云提供了 **密码安全中心(Data Encryption Workshop，简称DEW)**。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，防止密钥明文暴漏在 HSM 之外，从而防止密钥泄露。与华为云服务对接 KMS 的服务有 **对象存储服务(Object Storage Service，简称OBS)** 、云硬盘等。其次，专属加密满足租户更高合规性要求的加密场景，采用通过国家密码局认证或国际权威认证的硬件加密机，对租户业务进行 专属加密，默认双机架构以提高可靠性。最后，华为云多款存储产品如 EVS 、VBS 等均提供存储加密的机制。针对于传输中的数据，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**虚拟专用网络(Virtual Private Network，简称VPN)**和应用层 TLS 与证书管理，华为云服务为客户提供控制台和 API 两种访问方式，均采用加密传输协

编号	具体控制要求	客户关注点	华为云的应答
			议构建安全的传输通道，有效地降低数据在网络传输过程中被恶意嗅探的风险。 2. 客户对华为云的审计和监督权益会根据实际情况在双方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。
5.1.3.5 信息安全独立审查	**云服务客户** a) 云服务客户应要求提供书面证据，以证明云服务中信息安全控制措施和指导方针的实施情况与云服务提供商所作的声明相符。此类证据可包括针对相关标准的认证。 **云服务提供商** a) 云服务提供商应向云服务客户提供书面证据，以证实其已实施信息安全和个人数据保护的控制措施。 b) 当个别云服务客户的审计不可行或可能增加信息安全风险时，云服务提供商应提供独立证据，证明信息安全和个人数据保护已按照其政策和程序实施并运行。此类证据应在签订合同前向潜在的云服务客户提供。云服务提供商所选择的适当独立审计通常可作为满足云服务客户审查其运营需求的可接受方式，前提是提供了足够的透明度。当独立审计不可行时，云服务提供商应进行自我评估，并向云服务客户披露其评估过程和结果。	客户需要主动向提供商索取书面证据，以验证其宣称实施的信息安全控制措施和指导方针是否与实际情况相符。这类证据通常包括由第三方机构出具的、针对相关安全标准(如ISO 27001)的认证文件。	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。华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT服务管理等各个领域致力于为客户打造安全、可信的服务，为客户业务赋能增值、保驾护航。业务赋能增值、保驾护航。同时，华为云每年定期接受专业第三方审计机构的审核。如有必要，客户可以通过官方渠道向华为云申请获取证书以及审计报告的副本。

5.2 云基础设施与运营

5.2.1 人力资源安全

编号	具体控制要求	客户关注点	华为云的应答
5.2.1.1 安全意识培训	**云服务客户** a) 云服务客户应在针对云服务业务经理、云服务管理员、云服务集成商以及云服务用户(包括相关员工和承包商)的意识、教育和培训计划中增加以下内容： – 云服务使用标准和程序； – 与云服务相关的信息安全风险及其管理方式； – 使用云服务时的系统和网络环境风险； – 个人数据保护； – 适用的法律和监管事项。 b) 应向管理层及监督管理人员(包括各业务部门的管理人员)提供有关云服务的信息安全意识、教育和培训计划。 **云服务提供商** a) 云服务提供商应提供信息安全和个人数据保护方面的意识宣导、教育和培训，并要求承包商对云服务客户数据及云服务衍生数据的适当处理采取相同措施。此类数据可能包含对云服务客户而言属于机密的信息，或受到特定限制(包括监管限制)，对云服务提供商的访问和使用加以约束。	客户应对内外部云服务相关员工开展培训，培训内容应涵盖：云服务的使用标准与程序、相关的信息安全风险及管理方法、使用云服务时的系统与网络环境风险、个人数据保护以及适用的法律与监管事项。此外，客户还需向管理层及监督人员提供专门的信息安全意识与教育计划。	作为云服务提供商： 1. 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。 2. 华为云参照各类法规要求、监管要求、国际或行业标准建立了一套完善的信息安全和隐私保护管理体系，并持续改进。华为云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，并遵守各国《个人数据保护法》所述的数据保护原则。

5.2.2 资产管理

编号	具体控制要求	客户关注点	华为云的应答
5.2.2.1	**云服务客户**	客户的资产清单应涵盖	为配合客户满足监管要求，华为云

编号	具体控制要求	客户关注点	华为云的应答
资产目录	a) 云服务客户的资产清单应涵盖存储在云计算环境中的信息及相关资产。清单记录应标明资产的存放位置，例如云服务的标识。 **云服务提供商** a) 云服务提供商的资产清单应明确标识： - 云服务客户数据； - 云服务衍生数据。	存储在云计算环境中的信息及相关资产。清单记录应标明资产的存放位置，例如云服务的标识。	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。
5.2.2.2 信息分类	**云服务客户** a) 云服务客户应根据其采用的标签管理程序，对保存在云计算环境中的信息及相关资产进行标记。 **云服务提供商** a) 云服务提供商应记录并披露其提供的任何服务功能，以允许云服务客户对其信息及相关资产进行分类和标记。	客户应根据其采用的标签管理程序，对保存在云计算环境中的信息及相关资产进行标记。	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。

5.2.3 访问控制

编号	具体控制要求	客户关注点	华为云的应答
5.2.3.1 网络和网络服务的访问	**云服务客户** a) 云服务客户在使用网络服务时的访问控制策略应规定对所使用的每个独立云服务的用户访问要求。 **云服务提供商** /	客户在使用网络服务时的访问控制策略应规定对所使用的每个独立云服务的用户访问要求。	为配合客户满足监管要求，每一位华为云客户在华为云都拥有唯一可辨识的用户ID，并提供多种用户身份验证机制，包括账号密码、多因素认证等。**统一身份认证服务（Identity and Access Management，简称IAM）**支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。此外，IAM还支持客户的安全管理员设置登录策略，避免用户密码被暴力破解或者因为访问钓鱼页面等而导致账号信息泄露。IAM 同时支持多因子认

			证机制。多因子认证是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信认证码进行二次认证。用户修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。如果用户有安全可靠的外部身份认证服务商，可以将IAM服务的联邦认证外部用户映射成华为云的临时用户，并访问用户的华为云资源。IAM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。IAM可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来助力用户账户的安全。通过以上方式，实现对特权和紧急账号的有效管控。客户也可通过**云审计服务(Cloud Trace Service，简称CTS)**作为辅助，为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。
5.2.3.2 用户注册与注销	**云服务客户** a) 用户注册和注销程序应涵盖用户访问控制受到损害的情况，例如密码或其他用户注册数据遭到泄露或破坏(如因无意披露所致)。 **云服务提供商** a) 为管理云服务客户用户对云服务的访问，云服务提供商应向云服务客户提供用户注册和注销功能，以及这些功能的使用规范。	客户的用户注册和注销程序应涵盖用户访问控制受到损害的情况，例如密码或其他用户注册数据遭到泄露或破坏(如因无意披露所致)。	为配合客户满足监管要求，华为云通过**统一身份认证服务(Identity and Access Management，简称IAM)**构建“事前防御-事中阻断-事后审计”的全生命周期保护机制，满足用户访问控制受损(如密码泄露)的合规要求。在注册阶段，华为云协助客户强制执行高强度密码策略并开启多因素认证(MFA)，确保即使密码泄露，攻击者也无法通过单一凭证获取访问权；同时，利用态势感知(SA)和官方的访问密钥(AK/SK)泄露检测工具，系统能实时识别并自动限制异常凭证的权限，确保受损账户在注销或重置前无法造成进一步损害。在注销及应急响应流程中，华为云支持管理员通过管理控制台瞬间冻结受损用户、强制清理所有在线会话并作废

			相关访问密钥，确保访问权限被彻底、及时地回收。 此外，依托**云审计服务(Cloud Trace Service，简称CTS)**记录从注册到注销过程中的每一次关键操作，精准回溯密码泄露后的行为轨迹，确保用户注册数据在遭遇无意披露或恶意破坏时，依然具备完善的风险补救与恢复能力。
5.2.3.3 用户访问权限	**云服务客户** / **云服务提供商** a) 宋体云服务提供商应提供用于管理云服务客户的云服务用户访问权限的功能，以及这些功能使用规范。	无关注点。	每一位华为云客户在华为云都拥有唯一可辨识的用户ID，并提供多种用户身份验证机制，包括账号密码、多因素认证等。**统一身份认证服务(Identity and Access Management，简称IAM)**支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。此外，IAM还支持客户的安全管理员设置登录策略，避免用户密码被暴力破解或者因为访问钓鱼页面等而导致账号信息泄露。IAM 同时支持多因子认证机制。多因子认证是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信认证码进行二次认证。用户修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。如果用户有安全可靠的外部身份认证服务商，可以将IAM服务的联邦认证外部用户映射成华为云的临时用户，并访问用户的华为云资源。IAM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。IAM可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来助力用户账户的安全。通过以上方式，实现对特权和紧急账号的有效管控。客户也可通过**云审计服务**

			(Cloud Trace Service，简称CTS)作为辅助，为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。
5.2.3.4 特权访问权限管理	**云服务客户** a) 云服务客户应根据已识别的风险，采用足够的认证技术(例如，多因素认证)，以对云服务客户的云服务管理员访问云服务管理功能进行认证。 **云服务提供商** a) 云服务提供商应根据已识别的风险，为云服务客户方的云服务管理员提供足够的认证技术(例如，多因素认证)，以访问云服务的管理功能。	客户应根据已识别的风险，采用足够的认证技术(例如，多因素认证)，以对云服务客户的云服务管理员访问云服务管理功能进行认证。	华为云的**统一身份认证服务(Identity and Access Management，简称IAM)**为客户提供云上资源访问控制。IAM 同时支持多因子认证机制。多因子认证是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信认证码进行二次认证。用户修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。
5.2.3.5 用户密钥认证信息管理流程	**云服务客户** a) 云服务客户应验证云服务提供商在分配密码等秘密认证信息方面的管理程序是否满足云服务客户的自身要求。 **云服务提供商** a) 云服务提供商应提供有关云服务客户密钥认证信息管理流程的信息，包括此类信息的分配流程以及用户认证流程。	客户需应验证云服务提供商在分配密码等秘密认证信息方面的管理程序是否满足云服务客户的自身要求。	华为云提供了**密码安全中心(Data Encryption Workshop，简称DEW)**。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，防止密钥明文暴漏在 HSM 之外，从而防止密钥泄露。
5.2.3.6 信息访问控制	**云服务客户** a) 云服务客户应确保能够根据其访问控制策略限制对云服务中信息的访问，并实现此类限制。这包括限制对云服务、云服务功能以及在服务中维护的云服务客户数据的访问。 **云服务提供商**	客户应确保能够根据其访问控制策略限制对云服务中信息的访问，并实现此类限制。这包括限制对云服务、云服务功能以及在服务中维护的云服务客户数据的访问。	为配合客户满足权限分配的要求，华为云的**统一身份认证服务(Identity and Access Management，简称IAM)**为客户提供云上资源访问控制。使用IAM，客户管理员可以管理用户账号，并且可以控制这些用户账号对客户名下资源具有的操作权限。根据不同业务维度和相同业务不同职责，实行 RBAC权限管理。保证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。华为云内部人员的

	a) 云服务提供商应提供访问控制功能，使云服务客户能够限制对其云服务及在服务中维护的云服务客户数据的访问。		权限创建、变更及撤销均需经过指定人员的正式审批。所有运维账号，所有设备及应用的账号均实现统一管理，并通过统一审计平台集中监控，并且自动审计，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。账号管理员根据华为云内部规范的账号权限管理机制，对用户权限进行定期审核。
5.2.3.7 特权工具程序的运用	**云服务客户** a) 在允许使用实用程序的情况下，云服务客户应明确其云计算环境中将使用的实用程序，并确保这些实用程序不会干扰云服务的控制措施。 **云服务提供商** a) 云服务提供商应明确云服务中所使用任何实用程序的要求。云服务提供商应确保任何可绕过正常操作或安全程序的实用程序的使用仅限于授权人员，并应定期对这些程序的使用情况进行审查和审计。	客户应明确其云计算环境中将使用的实用程序，并确保这些实用程序不会干扰云服务的控制措施。	华为云的**统一身份认证服务(Identity and Access Management，简称IAM)**可允许客户的租户管理员灵活地进行用户权限管理，控制对云资源的创建、删除、修改、设置等操作的权限。此外，华为云通过**云审计服务(Cloud Trace Service，简称CTS)**为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。 同时，为配合客户满足监管的要求，IAM可以按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来助力用户账户的安全。通过以上方式，实现对特权和紧急账号的有效管控。客户也可通过CTS作为辅助，为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。
5.2.3.8 访问控制	**云服务客户** a) 云服务客户应要求其控制下的用户为任何账户遵循安全的登录程序。 **云服务提供商** a) 在需要时，云服务提供商应为云服务客户所要求的、由云服务客户控制的云服务用户账户提供安全的登录程序。	客户应要求其控制下的用户为任何账户遵循安全的登录程序。	华为云的**统一身份认证服务(Identity and Access Management，简称IAM)**为客户提供云上资源访问控制。使用IAM，支持客户的安全管理员设置登录策略，避免用户密码被暴力破解或者因为访问钓鱼页面等而导致账号信息泄露。IAM 同时支持多因子认证机制。多因子认证是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信认证码进行二次认证。用户修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。

5.2.4 密码学

编号	具体控制要求	客户关注点	华为云的应答
5.2.4.1 密码控制措施	**云服务客户** a) 云服务客户应为其使用实施密码控制措施，无论这些控制措施是由云服务客户自身提供还是由云服务提供商提供。 b) 当云服务提供商提供密码技术时，云服务客户应审查云服务提供商提供的相关信息，以确认其密码功能： – 是否满足云服务客户的策略要求； – 是否与云服务客户使用的其他密码保护措施兼容； – 是否适用于在云服务中处于静止状态以及在传入、传出和内部传输过程中的数据。 **云服务提供商** a) 云服务提供商应向云服务客户披露其用于保护所处理信息和个人数据的加密技术的相关信息。云服务提供商还应向云服务客户提供有关其提供的、可协助云服务客户实施自身密码保护功能的信息。	客户需识别 1.每个云服务的加密密钥，并实施密钥管理程序。 2.应审查云服务提供商提供的相关信息，以确认其密码功能是否满足策略要求；与使用的其他密码保护措施兼容；适用于在云服务中处于静止状态以及在传入、传出和内部传输过程中的数据。	为配合客户满足监管要求 1. 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。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. 华为云服务端加密功能还集成了**密码安全中心(Data Encryption Workshop，简称DEW)**的密钥管理功能，由DEW进行密钥全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，确保了客户云上数据的安全。DEW采用分层密钥管理机制，方便各层密钥的轮换。通过DEW的控制台或API进行关联设置，各存储服务加密数据时使用的加密密钥，能够由保存在DEW中的客户主密钥进行加密，该客户主密钥又由保存在硬件安全模块HSM中的根密钥进行加密，构成了一条完整的安全、可信的密钥链，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取根密钥。 3. 华为云在信息传输过程中使用安全的加密通道(如HTTPS)，对存储的静态数据使用安全的加密算法，确保不同状态下的数据机密性。通过数字签名、时间戳等控制机制，防止数据传输过程中的篡改，保证信息的完整性，以及防止重放攻击。记录应用服务中的操作日志，以此来支持审计。对接口进行身份认证、传输和边界保护，确保API应用的安全。

编号	具体控制要求	客户关注点	华为云的应答
5.2.4.2 密钥管理	**云服务客户** a) 云服务客户应识别每个云服务的加密密钥，并实施密钥管理程序。 b) 当云服务向云服务客户提供密钥管理功能时，云服务客户应要求获取与该云服务相关的密钥管理所采用程序的以下信息： – 密钥类型； – 密钥管理系统的技术规范，包括密钥生命周期各阶段的程序，即生成、变更或更新、存储、停用、检索、保留和销毁； – 建议云服务客户采用的密钥管理程序。 c) c) 当云服务客户采用其自身的密钥管理时，不应允许云服务提供商存储和管理用于加密操作的密钥。 **云服务提供商** /	1. 客户应识别每个云服务的加密密钥，并实施密钥管理程序，获取与该云服务相关的密钥管理所采用程序信息。 2. 当客户采用其自身的密钥管理时，不应允许云服务提供商存储和管理用于加密操作的密钥。	华为云提供了**密码安全中心(Data Encryption Workshop，简称DEW)**。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)为客户创建和管理密钥，拥有主流国际安全认证，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。

5.2.5 物理安全与环境安全

编号	具体控制要求	客户关注点	华为云的应答
5.2.5.1 数据中心地址	**云服务客户** 应使用位于泰国的主要数据中心。 **云服务提供商** a) 主数据中心应位于泰国。 b) 云服务提供商应在泰国或东南亚区域内，尽可能在地理位置上靠近云服务客户主要运营地点的位置建立次要(备份)数据中心，包括新加坡以及中华人民共和国香港特别行政区。	客户需使用位于泰国的主要数据中心。	1. 华为云以区域为单位提供服务，区域也即是客户内容数据的存储位置，华为云未经授权绝不会跨区域移动客户的内容数据。客户在使用云服务时，依据就近接入原则、不同地域的适用的法律法规要求等进行区域的选择，使客户内容数据存储在目标位置。当客户使用云硬盘、对象存储、云数据库、容器引擎等服务时，华为云通过卷、存储桶、数据库实例、容器等不同粒度的访问控制机制，使客户只能访问到自

编号	具体控制要求	客户关注点	华为云的应答
			己的数据。 2. 在泰国，华为云已部署“亚太-曼谷”Region，拥有3个可用区(AZ)。在新加披，华为云已部署“亚太-新加披”Region，拥有4个可用区(AZ)。在中国香港，华为云已部署“中国-香港”Region，拥有4个可用区(AZ)，详情见华为云官网“**全球基础设施**”。
5.2.5.2 资源安全处置	**云服务客户** a) 云服务客户应要求确认云服务提供商具备资源安全处置或重复使用的政策和程序。 **云服务提供商** a) 云服务应确保及时对资源(例如设备、数据存储、文件、内存)的安全处置或再利用做出安排。 b) 为实现安全处置或再利用，凡包含可能存有个人数据的存储介质的设备，均应视为确实含有此类数据，并应以确保数据无法被恢复的方式进行安全处置或为再利用做好准备。	客户应要求确认云服务提供商具备资源安全处置或重复使用的政策和程序。	为配合客户满足监管要求 1. 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，并遵守各国《个人数据保护法》所述的数据保护原则。此外，华为云各服务产品和组件从设计之初就规划并实现了隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。 2. 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。 3. 针对于数据安全删除，华为云

编号	具体控制要求	客户关注点	华为云的应答
			在客户确认删除数据后，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。

5.2.6 运营安全

编号	具体控制要求	客户关注点	华为云的应答
5.2.6.1 变更管理	**云服务客户** a) 云服务客户的变更管理流程应考虑云服务提供商所做任何变更的影响。 **云服务提供商** a) 云服务提供商应向云服务客户通报可能对云服务产生不利影响的变更信息。以下信息将有助于云服务客户评估变更对信息安全造成的影响： – 变更的类别； – 变更的计划日期和时间； – 对云服务及底层系统所做变更的技术说明； – 变更开始和完成的通知。 b) 当云服务提供商所提供的云服务依赖于另一家对等云服务提供商时，该云服务提供商可能需要向云服务客户通报由对等云服务提供商引起的变更。	客户的变更管理流程应考虑云服务提供商所做任何变更的影响。	为配合客户遵从监管要求，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。 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。同时，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。 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

编号	具体控制要求	客户关注点	华为云的应答
			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。
5.2.6.2 容量管理	**云服务客户** a) 云服务客户应确保云服务提供商所约定的容量满足云服务客户的需求。 b) 云服务客户应监控云服务的使用情况，并预测资源容量需求，以确保云服务在一段时间内的性能表现。 **云服务提供商** a) 云服务提供商应监控总资源容量，以防止因资源短缺导致的信息安全事件。	客户应确保云服务提供商所约定的容量满足云服务客户的需求，监控云服务的使用情况，并预测资源容量需求，以确保云服务在一段时间内的性能表现。	为配合客户遵从监管要求，华为云制定了规范的容量管理及资源预测程序，对华为云容量进行统筹管理，提升华为云资源可用性服务水平。根据各方的输入，滚动预测未来资源容量，制定合适的资源扩容方案，并每天定期监控华为云的容量使用情况，分析评估业务容量瓶颈及性能瓶颈，在资源达到预设阈值时，发布资源预警，进而采取进一步解决方法，避免对租户云服务的系统性能造成影响。 同时，华为云的**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。云监控服务提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。
5.2.6.3 信息备份	**云服务客户** a) 当云服务提供商将备份功能作为云服务的一部分提供时，云服务客户应向云服务提供商索取备份功能的详细规格，并验证其是否满足自身的备份需求。 b) 当云服务提供商未提供备份功能时，云服务客户有责任自行实施备份能力。 **云服务提供商** a) 云服务提供商应向云服务客户明示其备份能力的详细说明。相关说明应视情况包括以下信息： – 备份的范围和时间安排； – 备份方法和数据格式，如适用，包括加密方式；	客户应向云服务提供商索取备份功能的详细规格，并验证其是否满足自身的备份需求。当云服务提供商未提供备份功能时，云服务客户有责任自行实施备份能力。	为配合客户遵从监管要求 1. 华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。客户可以使用对象存储服务的版本控制、云硬盘备份、云服务器备份等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云。更多云备份信息可参考华为云备份官网**云备份 (Cloud Backup and Recovery，简称CBR)**。 2. 华为云的**统一身份认证服务(Identity and Access Management，简称IAM)**为客户提供云上资源访问控制。IAM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

编号	具体控制要求	客户关注点	华为云的应答
	– 备份数据的保留期限； – 验证备份数据完整性的程序； – 从备份中恢复数据的相关程序和时间要求； – 测试备份能力的程序； – 备份的存储位置。 b) 若向云服务客户提供此类服务，云服务提供商应提供安全且隔离的备份访问权限。		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。IAM可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来助力用户账户的安全。
5.2.6.4 事件日志	**云服务客户** a) 云服务客户应定义其事件日志记录的需求，并验证云服务是否满足这些需求。 **云服务提供商** a) 云服务提供商应向云服务客户提供建立日志的功能。 b) 在适用的情况下，事件日志应记录事件是否导致个人数据被更改(即添加、修改或删除)，并识别出相关责任人(审计日志)。当在参考云架构中涉及多个云服务提供商共同提供服务时，应明确界定满足此要求的角色和责任，且该责任可由多方共同承担。	客户应定义其事件日志记录的需求，并验证云服务是否满足这些需求。	为配合客户满足监管要求 1. 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。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。 2. 华为云明确定义了与客户之间的安全责任共担模型，具体查阅本文第三章。
5.2.6.5 日志信息保护	**云服务客户** a) 出于安全监控和运行诊断等目的所记录的日志信息可能包含个人数据。应采取措施(例如控制访问权限)，以确保日志信息仅用于其预定目的。 b) 应建立一种程序，以确保日志信息在规定的保留期限内被删除，并保留相关记录。	1.客户应采取措施(例如控制访问权限)，以确保日志信息仅用于其预定目的。 2.应建立一套程序，以确保日志信息在规定的保留期限内被删除，并保留相关记录。	1. 华为云的**云日志服务 (Log Tank Service，简称LTS)**结合**统一身份认证服务(Identity and Access Management，简称IAM)**和**对象存储服务(Object Storage Service，简称OBS)**，可以全面满足客户对日志安全与生命周期管理的需求。 2. 访问控制与预定目的使用**云日志服务 (Log Tank Service，简**

编号	具体控制要求	客户关注点	华为云的应答
	云服务提供商 a) 出于安全监控和运行诊断等目的所记录的日志信息可能包含个人数据。应采取措施(例如控制访问权限)，以确保日志信息仅用于其预定目的。 b) 应建立一种程序，以确保日志信息在规定的保留期限内被删除，并保留相关记录。		**称LTS)**通过IAM 进行精细的权限管理，以达到不同员工之间的权限隔离。客户可以使用IAM为员工创建用户，并通过策略精确控制其对LTS资源的访问范围，例如授予仅能使用日志但禁止删除等高危操作的权限。这确保了包含个人数据的日志信息仅被授权人员访问，用于安全监控和运行诊断等预定目的。同时，LTS自身也通过HTTPS传输加密和日志冗余存储等技术手段保障数据在传输和存储过程中的安全性。 3. 自动化的日志生命周期管理。LTS提供了内置的日志存储时间(保留期限)管理功能。客户在创建或管理日志流时，可以设置日志的存储时间(支持在1~30天之间)。系统会根据设置的日志存储时间自动清理过期的日志数据，这实现了程序化(自动)的删除机制。对于需要长期保留的日志，LTS支持将日志转储至**对象存储服务(Object Storage Service，简称OBS)** 进行长期存储。OBS本身也提供生命周期策略，可以进一步自动化管理数据的归档与删除。所有转储、删除等操作均可通过**云审计服务(Cloud Trace Service，简称CTS)**记录，从而保留相关操作记录以供审计。
5.2.6.6 管理员和操作员日志	**云服务客户** a) 如果将特权操作委托给云服务客户，则应记录该操作及其执行情况。云服务客户应确定云服务提供商提供的日志记录功能是否合适，或是否需要由云服务客户实施额外的日志记录功能。 **云服务提供商**	客户应记录该操作及其执行情况，确定云服务提供商提供的日志记录功能是否合适，或是否需要由云服务客户实施额外的日志记录功能。	为配合客户满足监管要求，可使用华为云的**云审计服务(Cloud Trace Service，简称CTS)**和**云日志服务(Log Tank Service，简称LTS)**功能。CTS能自动记录所有用户(包括云服务客户)对云资源的操作，包括特权操作及其执行情况。客户可通过CTS查询7天内的操作记录，并可将日志转储至**对象存储服务(Object Storage Service，简称OBS)**或LTS进行长期存储和分析。同时，LTS

编号	具体控制要求	客户关注点	华为云的应答
	/		提供强大的日志采集、存储、搜索和分析能力，支持从主机、容器等多种来源采集日志。客户可评估CTS的内置功能是否合适，并根据需要利用LTS实施额外的日志记录功能。
5.2.6.7 时钟同步	**云服务客户** a) 云服务客户应请求获取有关云服务提供商系统所使用时钟同步的信息。 **云服务提供商** a) 云服务提供商应向云服务客户提供其系统所使用的时钟信息，并提供客户如何将其本地时钟与云服务时钟同步的相关信息。	客户应请求获取有关云服务提供商系统所使用时钟同步的信息。	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，使得通信设备与通信网的时钟同步，确保系统内各网元时间的一致性。
5.2.6.8 技术漏洞管理	**云服务客户** a) 云服务客户应向云服务提供商索取有关可能影响所提供云服务的技术漏洞管理情况的信息。云服务客户应明确其负责管理的技术漏洞，并明确定义管理这些漏洞的流程。 **云服务提供商** a) 云服务提供商应向云服务客户提供可能影响所提供云服务的技术漏洞管理相关信息。	客户应向云服务提供商索取有关可能影响所提供云服务的技术漏洞管理情况的信息。明确其负责管理的技术漏洞，并明确定义管理这些漏洞的流程。	华为云产品安全事件响应团队(CSIRT)已经建立成熟的漏洞响应机制，针对华为云的自运营的特点，通过持续优化安全漏洞的管理流程和技术手段，以保证基础设施、平台、应用和云服务中的自研和第三方漏洞尽快修复，降低对用户业务造成影响的风险。同时，华为CSIRT和华为云安全运维团队已经建立了漏洞感知、处置和对外披露的机制。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，降低并最终避免漏洞被恶意利用而导致影响用户业务的风险。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用户业务造成影响。
5.2.6.9 开发、测试和运营环	**云服务客户** a) 若无法避免将个人数据用于测试目的，应进行风险评估，并实施技术和组织措施以将已识别的风险降至最低。	客户若无法避免将个人数据用于测试目的，应进行风险评估，并实施技术和组织措施以将已识别的风险降至最低。	华为云避免将生产数据用于测试，如需使用生产数据进行测试，必须经过脱敏，使用完成后需要进行数据清理。华为云参照各类法规要求、监管要求、国际或行业标准建立了信息安全风险评估方法，若无法避免将个人数据用于测试目的，

编号	具体控制要求	客户关注点	华为云的应答
境的分离	**云服务提供商** 若无法避免将个人数据用于测试目的，则应进行风险评估，并实施技术和组织措施以将已识别的风险降至最低。		将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，同时根据要求执行信息安全风险评估。

5.2.7 通信安全

编号	具体控制要求	客户关注点	华为云的应答
5.2.7.1 信息传输制度和程序	**云服务客户** a) 在使用物理介质进行信息传输时，应建立系统以记录包含个人数据的进出物理介质，包括物理介质的类型、授权的发送方/接收方、日期和时间以及物理介质的数量。 b) 云服务客户应要求云服务提供商采取额外措施(例如加密)，以确保数据只能在目的地被访问，而在传输过程中无法被访问。 **云服务提供商** a) 在使用物理介质进行信息传输时，应建立系统以记录包含个人数据的进出物理介质，包括物理介质的类型、授权的发送方/接收方、日期和时间以及物理介质的数量。 b) 在可行的情况下，应要求云服务客户采取额外措施(例如加密)，以确保数据只能在目的地被访问，而在传输过程中无法被访问。	客户在使用物理介质传输个人信息时，共同建立记录系统，并优先采取加密等安全措施。具体包括建立记录系：双方均应建立系统，详细记录包含个人数据的进出物理介质信息，如介质类型、授权收发方、日期时间及数量。 强化传输安全：在可行情况下，双方应要求对方采取额外措施(例如加密)，确保数据只能在目的地被访问，在传输过程中无法被访问。	1. 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. 针对于传输中的数据，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**虚拟专用网络(Virtual Private Network，简称 VPN)**和应用层 TLS 与证书管理，华为云服务为客户提供控制台和 API 两种访问方式，均采用加密传输协议构建安全的传输通道，有效地降低数据在网络传输过程中被恶意嗅探的风险。
5.2.7.2 网络隔离	**云服务客户** a) 云服务客户应定义其在网络隔离方面的需求，以在云服务的共享环境中实现租户隔离，并验证云服务提供商是否满足这些需求。	客户应定义其在网络隔离方面的需求，以在云服务的共享环境中实现租户隔离，并验证云服务提供商是否满足这些需求。	1. 华为云为客户提供的**虚拟私有云 (Virtual Private Cloud，简称VPC)**服务可为租户构建出私有网络环境，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络

编号	具体控制要求	客户关注点	华为云的应答
	云服务提供商 a) 云服务提供商应针对以下情况实施网络访问隔离：在多租户环境中实现租户之间的隔离；实现云服务提供商内部管理环境与云服务客户云计算环境之间的隔离。 b) 在适当情况下，云服务提供商应协助云服务客户验证云服务提供商所实施的隔离措施。		ACL和安全组规则，对进出子网以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。 2. 华为云各服务产品和组件从设计之初就规划并实现了隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。

5.2.8 系统获取、开发和维护

编号	具体控制要求	客户关注点	华为云的应答
5.2.8.1 信息安全需求分析与规范	**云服务客户** a) 云服务客户应确定其对云服务的信息安全需求，然后评估云服务提供商所提供的服务是否能够满足这些需求。 b) 为进行此项评估，云服务客户必须向云服务提供商索取有关信息安全能力的信息。 **云服务提供商** a) 云服务提供商应向云服务客户提供与其所使用的信息安全能力相关的信息。此类信息应具有说明性，但不得披露可能对怀有恶意意图的人员有用的信息。	客户应确定其对云服务的信息安全需求，然后评估云服务提供商所提供的服务是否能够满足这些需求。	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提出的获取信息的要求。华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT服务管理等各个领域致力于为客户打造安全、可信的服务，为客户业务赋能增值、保驾护航。业务赋能增值、保驾护航。同时，华为云每年定期接受专业第三方审计机构的审核。如有必要，客户可以通过官方渠道向华为云申请获取证书以及审计报告的副本。
5.2.8.2 安全开发制度	**云服务客户** a) 云服务客户必须向云服务提供商请求有关其使用安全开发程序和实践的信息。 **云服务提供商** a) 云服务提供商必须根据其	客户必须向云服务提供商获取有关其使用安全开发程序和实践的信息。	为配合客户满足监管要求，华为云作为云服务提供商，遵守网络安全要求，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。此外，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

编号	具体控制要求	客户关注点	华为云的应答
	信息披露政策，提供有关其采用安全开发流程和实践的信息。		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。 • 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。

5.2.9 供应商关系

编号	具体控制要求	客户关注点	华为云的应答
5.2.9.1 供应商关系信息安全政策	**云服务客户** a) 云服务客户应在与其供应商关系相关的信息安全策略中，将云服务提供商列为一种供应商类型。这将有助于降低与云服务提供商对云服务客户数据的访问和管理相关的风险。 **云服务提供商** /	客户应在与其供应商关系相关的信息安全策略中，将云服务提供商列为一种供应商类型。	为配合客户满足监管要求，华为云作为云服务提供商，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。华为云使用多种隐私保护平台工具，帮助华为云更快速、系统、高效地处理与隐私保护相关的各项工作。
5.2.9.2供应商协议中的安全保障	**云服务客户** a) 云服务客户应确认服务协议中所述与云服务相关的信息安全角色和责任。这些责任可能包括以下流程： - 恶意软件防护； - 备份； - 加密控制； - 漏洞管理； - 事件管理； - 技术合规性检查； - 安全测试； - 审计； - 日志和审计轨迹等证据的收集、维护和保护； - 服务协议终止时信息的保护； - 身份验证和访问控制； - 身份和访问管理。 **云服务提供商** a) 云服务提供商应在协议中明确说明其将实施的相关信息安全措施，以确保云服务提供商与云服务客户之间不存在误	客户与提供商需在服务协议中明确界定双方的信息安全角色与责任，以构建清晰的责任共担模型。	华为云提供了线上的**《华为云用户协议》**以及**《云服务等级协议》**，其中规定了所提供服务内容和服务水平，以及客户和华为云的安全职责。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。

编号	具体控制要求	客户关注点	华为云的应答
	解。这些措施可包括以下流程： – 恶意软件防护； – 备份； – 加密控制； – 漏洞管理； – 事件管理； – 技术合规性检查； – 安全测试； – 审计； – 日志和审计追踪等证据的收集、维护与保护； – 服务协议终止时的信息保护； – 身份验证与访问控制； – 身份和访问管理。 b) 云服务提供商将实施的相关信息安全措施，可根据云服务客户所使用的云服务类型而有所不同。		
5.2.9.3 信息和通信技术供应链	**云服务客户** / **云服务提供商** a) 如果云服务提供商使用其他对等云服务提供商的云服务，该云服务提供商应确保对其自身云服务客户的信息安全水平保持不变或进一步提高。 b) 当云服务提供商基于供应链提供云服务时，应向供应商明确信息安全目标，并要求各供应商开展风险管理活动以实现这些目标。	客户应关注云服务提供商是否有效管理其供应商。	华为云已建立供应商管理体系，维护符合资质的供应商采购名单，在供应商引入前会进行尽职调查，签署合同、服务协议、保密协议，约定双方责任与义务、服务水平等要求，供应商引入后每年对供应商的安全风险进行评估及安全稽查。

5.2.10 信息安全事件管理

编号	具体控制要求	客户关注点	华为云的应答
5.2.10.1 职责和	**云服务客户** a) 云服务客户应核实信息安	客户应核实信息安全事件管理责任的分配情	华为云作为服务提供商： 1. 华为云作为客户的服务提供

编号	具体控制要求	客户关注点	华为云的应答
程序	全事件管理责任的分配情况，并确保其满足要求。 b) 发生信息安全事件时，云服务客户应根据其信息安全事件管理流程，单独或与云服务提供商共同开展审查，以确定是否发生了个人数据泄露事件。 **云服务提供商** a) 作为服务规范的一部分，云服务提供商应明确界定云服务客户与云服务提供商之间在信息安全事件管理方面的责任划分和处理程序。 b) 云服务提供商应向云服务客户提供以下方面的书面文件： – 云服务提供商将向云服务客户报告的信息安全事件的范围； – 信息安全事件的检测情况及其相关响应措施的披露程度； – 信息安全事件通知的目标时间范围； – 信息安全事件通知的程序； – 处理与信息安全事件相关问题的联系信息； – 在发生特定信息安全事件时可采取的补救措施。 c) 一旦发生信息安全事件，云服务客户应根据其信息安全事件管理流程进行审查，或由云服务客户与云服务提供商共同审查，以确定是否发生了个人数据泄露事件。	况，并确保其满足要求。 发生信息安全事件时，应根据其信息安全事件管理流程，单独或与云服务提供商共同开展审查，以确定是否发生了个人数据泄露事件。	方，会安排专人积极配合的安全事件调查。华为云专业的服务工程师团队提供 7*24小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等联络到华为云的支持团队。 2. 华为与安全管理部门负责制定和执行华为端到端网络安全保障体系与安全策略，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。 3. 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。
5.2.10.2 汇报信息安全事件	**云服务客户** a) 云服务客户应向云服务提供商请求有关以下机制的信息：云服务客户向云服务提供商报告其检测到的信息安全事件的机制；云	客户应向云服务提供商提供其检测到的信息安全事件的机制；云服务提供商接收其自身检测到的信息安全事件报告的机制；云服务客户跟踪已报告的信息安全事	作为云服务提供商： 1. 华为云作为认可机构的服务提供方，会积极配合认可机构主动发起的沟通。华为云专业的服务工程师团队提供 7*24小时的服务支持，客户可以通过工

编号	具体控制要求	客户关注点	华为云的应答
	服务提供商接收其自身检测到的信息安全事件报告的机制；云服务客户跟踪已报告的信息安全事件处理状态的机制。 **云服务提供商** a) 云服务提供商应提供以下机制： 供云服务客户向云服务提供商报告信息安全事件；供云服务提供商向云服务客户报告信息安全事件；供云服务客户跟踪已报告的信息安全事件的处理状态。	件处理状态的机制。	单、智能客服、自助服务、热线电话等联络到华为云的支持团队。 2. 华为云也根据内部业务连续性管理体系的要求，制定了危机沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。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。 3. 华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。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。

6 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

	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

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

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

7 结语

华为云致力于为泰国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，有助于泰国云用户详细了解华为云对于金融行业监管要求方面的遵从性，让客户安全、放心地使用华为云。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合泰国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。

8 版本历史

日期	版本	描述
2026 年 5 月	1.0	首次发布