华为云印度尼西亚网络安全监管要求遵从性指南

文档版本 1.0

发布日期 2022-12-26

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

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，通信和信息技术部（Kominfo）、众议院（DPR）、印尼法律和人权部（Ministry of Law and Human Rights）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印度尼西亚网络安全监管要求，详细阐述华为云将如何协助其满足这些监管要求。

1.2 适用的印度尼西亚网络安全的监管要求简介

- **2008年第11号法规《电子信息和交易法》（Law No.11 of 2008 on Electronic Information and Transaction）**2008年4月21日，印尼政府发布了该法规，在电子信息、记录、签名、电子系统和电子认证的实施提供、电子交易、域名、知识产权、隐私保护权等方面提出了要求。
- **2016年第19号法规- 关于2008年第11号《电子信息和交易法》的修正案（Law No. 11 of 2008 on Electronic Information and Transaction as amended by Law No.19 of 2016）**2016年11月25日，印尼政府发布了2008年第11号《电子信息和交易法》的修正案。
- **2019年第71号条例《关于电子系统和交易的实施》（Government Regulation No.71 of 2019 Regarding the Provision of on Electronic System and Transaction）**2019年10月10日，印度尼西亚法律和人权部发布了该条例，在电子系统运营、电子代理商、电子交易操作、电子认证操作、可靠性认证机构、域名管理等方面提出了要求。该条例取代了2012年关于实施《电子系统和交易法》的第82号政府条例。
  - Kominfo**2020年第5号条例《关于私营电子系统供应商》（Minister of Communication and Informatics Regulation No.5 of 2020 on Private Electronic System Providers）**2020年11月24日，通信和信息技术部发布了该条例，规定私营电子系统运营商的注册，电子信息或电子文件的管理、审核，并要求断开私营电子系统运营商对禁用电子违禁信息或文件的访问。

- **Kominfo2021年第10号条例-第2020年5号条例《关于私营电子系统供应商》的修正案（Kominfo Regulation No. 10 of 2021 - Amendment to Regulation No. 5 of 2020（on private electronic system providers））**
  2021年5月21日，通信和信息技术部发布了2021年第10号条例《关于私营电子系统供应商》的修正案。
- **Kominfo2007年第26号条例《关于互联网协议的电信网络使用安全》（Kominfo Regulation No. 26 of 2007（on the security of the use of telecommunications networks for Internet Protocol）**2007年5月4日，通信和信息技术部发布了该条例，主要针对使用互联网协议的电信运营商提出要求。
- **Kominfo2017年第5号条例-对Kominfo第26/2007号条例的修正案（Kominfo Regulation No. 5 of 2017 - Amendments to Kominfo Regulation No. 26/2007）**2017年1月24日，通信和信息技术部发布了《关于互联网协议的电信网络使用安全》的修正案。

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。
- **客户**

  指与华为云达成商业关系的注册用户。
- **云计算**

  云计算是一种基于可快速配置和发布，并且具有最少的服务配置管理或交互能力的网络、服务器、存储、应用程序和服务的共享需求，能够提供公平、简单和按需访问的计算模型。
- **服务提供商**

  根据外包安排向金融机构提供服务的实体以及实体的分支机构。
- **电子信息**

  电子信息是一个或一组电子数据，包括但不限于文字、声音、图片、地图、设计、照片、电子数据交换（EDI）、电子邮件（电子邮件）、电报、电传、传真或类似的，经过处理的字母、符号、数字、访问代码、符号或穿孔，它们具有意义或能够被能够理解它们的人理解。
- **电子系统**

  电子系统是一系列用于准备、收集、处理、分析、存储、显示、公布、传输和/或传播电子信息的电子设备和程序。
- **电子代理**

  电子代理是来自电子系统的设备，用于对由个人自动组织的特定电子信息执行操作。
- **电子交易**

  电子交易是使用计算机、计算机网络和/或其他电子媒体进行的法律行动。
- **电子系统运营商**

  电子系统运营商是为电子系统用户自己的需要和/或其他方的需要单独或联合提供、管理和/或操作电子系统的任何个人、州管理员、商业实体和社区。
- **私营电子系统运营商**

私营电子系统运营商是个人、商业实体和公众的电子系统运营商

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，华为云已获得众多国际和行业安全合规资质认证，全力保障客户部署业务的安全，主要包括：

全球性标准类认证

认证	描述
ISO20000-1:2011	ISO20000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。
ISO27001:2013	ISO27001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。
ISO27017:2015	ISO27017是针对云计算信息安全的国际认证。ISO27017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。
ISO22301:2012	ISO22301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。
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。
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。

认证	描述
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。
国际通用准则CCEAL3+	CC(Common Criteria)认证是一种信息技术产品和系统安全性的评估标准，它提供了一组通用的安全功能要求和安全保证要求，并在这些保证要求的基础上提供衡量IT安全性的尺度（即评估保证级EAL），使得独立的安全评估结果可以互相比较。
ISO27018:2014	ISO27018是专注于云中个人数据保护的国际行为准则。ISO27018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。
ISO29151:2017	ISO29151是国际个人身份信息保护实践指南。ISO29151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。
ISO27701:2019	ISO27701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ISO27701表明了其在个人数据保护具有健全的体制。
BS10012:2017	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。
M&O认证	Uptime Institute是目前全球公认的数据中心标准化组织和权威的专业认证机构。华为云数据中心已获得Uptime Institute颁发的全球顶级数据中心基础设施运维认证(M&O认证)。获得M&O认证象征着华为云数据中心运维管理已处于国际领先水平。
NIST网络安全框架(CSF)	NIST CSF由标准、指南和管理网络安全相关风险的最佳实践三部分组成，其核心内容可以概括为经典的IPDRR能力模型，即风险识别能力（Identify）、安全防御能力（Protect）、安全检测能力（Detect）、安全响应能力（Response）和安全恢复能力（Recovery）五大能力。
PCI 3DS认证	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。

地区性标准类认证

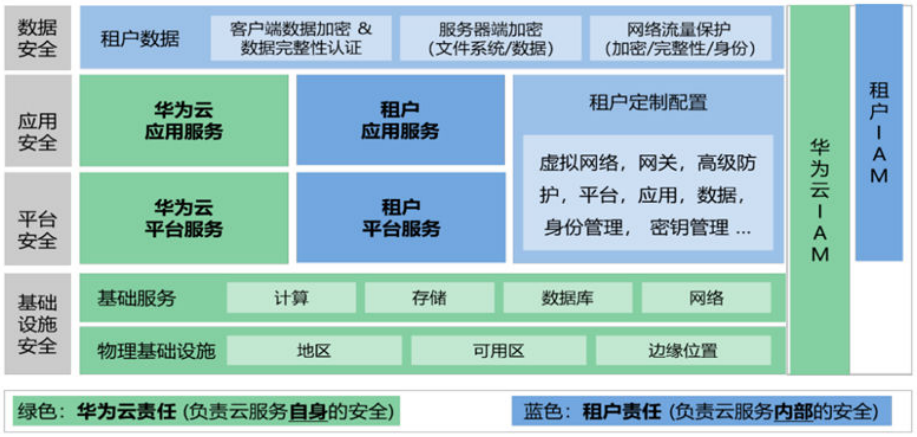
认证	描述
中国网络安全等级保护	网络安全等级保护是中华人民共和国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为中国各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键Region、节点通过了网络安全等级保护四级。
新加坡MTCS Level3 认证	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level3等级认证。
中国可信云金牌运维专项评估	金牌运维评估是面向已通过中国可信云服务认证的云服务供应商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、健全的运维管理体系，符合中国权威云服务运营和维护保障要求的认证标准。
中国云服务用户数据保护能力认证	云服务用户数据保护能力评估是针对云服务用户数据安全的评估机制，评测关键指标范围包括事前防范、事中保护、事后追溯三个层面。
中国工信部云计算服务能力评估	云计算服务能力评估是以《信息技术云计算云服务运营通用要求》等相关中国国家标准为依据的分级评估标准。华为私有云和公有云双双获得云计算服务能力“一级”符合性证书。
中国可信云评估	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。
中国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。华为云服务政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。

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**”。

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。

图 3-1 责任共担模型



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、数据层和用户身份管理（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 华为云如何遵从 2008 年第 11 号法规《电子信息和交易法》及其修正案

印尼政府在2008年4月21日发布了《电子信息和交易法》，该法规在电子信息、记录、签名、电子系统和电子认证的实施提供、电子交易、域名、知识产权、隐私保护权等方面提出了要求。2016年11月25日，印尼政府发布了《电子信息和交易法》的修正案。

以下内容将总结《电子信息和交易法》中与云服务供应商相关的控制要求，并详细阐述了华为云的内部实践，以及华为云作为云服务提供商，如何帮助客户满足这些控制要求。

5.1 实施电子认证和电子系统

编号	具体控制要求	华为云的内部实践	客户的关注点
电子系统的实施 第15条 第15条	（1）任何电子系统运营商（PSE）必须以可靠和安全的方式提供电子系统，并应对电子系统的正常运行负责。 （2）电子系统运营商应负责提供电子系统。 （3）如果电子系统用户发生不可抗力的情况、过失和/或疏忽，则第（2）款所拟的规定不适用。	华为云应遵从所有适用的国家和地区的安全法规政策、国际网络安全和云安全标准，在参考行业最佳实践的基础上，从组织、流程、规范、技术、合规、生态等方面建立并完善高可信、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透明的方式，共同应对云安全挑战，全面满足云服务用户的安全需求。	客户（电子系统运营商）应对电子系统正常运行负责，保证信息在系统中的可用性、完整性、机密性、真实性和可访问性、保证业务连续性。

电子系统的实施 第16条	（1）除非法律另有规定，任何电子系统运营商均须按照以下最低要求运营电子系统： a.可以按照法律法规规定的保留期重新显示电子信息和/或电子记录的全部; b. 运营电子系统时，能够保护电子信息的可用性、完整性、真实性、保密性和可访问性; c.可按照提供电子系统的程序或说明运作; d.提供语言、信息或符号可被电子系统运营方所理解的程序或说明;和 e.采用可持续机制，以便保持程序或说明的时效性、明确性和问责制。 （2）有关提供电子系统运营的进一步规定应由政府条例管理。	华为作为云服务提供商，提供云硬盘、对象存储等多种存储服务，客户可依据法律法规要求自行设定数据的保留期限。此外，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，充分利用云服务模式下按需使用、弹性扩展、可靠性高的特点，结合备份归档软件和华为云基础设施，将客户云下数据备份归档到华为云。 华为云保护租户数据的机密性、完整性、可访问性等方面的全面数据保护功能，并对相关功能的安全性负责。华为云绝不允许运维人员在未经授权的情况下访问租户数据。 华为云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。各可用区应有各自独立的UPS和现场备用发电设备，所有可用区域与多个一级传输供应商冗余相连，排除单点故障的风险。	客户（电子系统运营商）应按照法规要求保留日志记录，保证信息在系统中的可用性、完整性、机密性、真实性和可访问性、保证业务连续性。以印尼语提供服务使用说明，并结合内外部法规要求的变化，保证管理要求持续更新。 为配合客户满足日志管理监管要求，华为云提供**云日志服务（Log Tank Service，简称LTS）**具备日志收集、实时查询、转储等功能，可长期保存日志。主机和云服务的日志数据上报至LTS后，存储时间可以在1-30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）、数据接入服务（DIS）中长期保存。

6 华为云如何遵从 2019 年第 71 号条例《关于电子系统和交易的实施》

印尼法律和人权部在2019年10月10日发布了2019年第71号政府条例《关于电子系统和交易的实施》，在电子系统运营、电子代理商、电子交易操作、电子认证操作、可靠性认证机构、域名管理等方面提出了要求。

以下内容将总结《关于电子系统和交易的实施》中与云服务供应商相关的控制要求，并详细阐述了华为云的内部实践，以及华为云作为云服务提供商，如何帮助客户满足这些控制要求。

6.1 电子系统运营

编号	具体控制要求	华为云的内部实践	客户的关注点
通用条例 第3条	（1）每个电子系统运营商必须可靠、安全地运营电子系统，并对电子系统的正确操作负责。 （2）电子系统运营商负责电子系统的实施。 （3）第（2）款所述的规定不适用于能够证明电子系统用户不可抗力、错误和/或疏忽的情况。	华为云应遵从所有适用的国家和地区的安全法规政策、国际网络安全和云安全标准，在参考行业最佳实践的基础上，从组织、流程、规范、技术、合规、生态等方面建立并完善高可信、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透明的方式，共同应对云安全挑战，全面满足云服务用户的安全需求。	客户（电子系统运营商）应对电子系统正常运行负责，保证信息在系统中的可用性、完整性、机密性、真实性和可访问性、保证业务连续性。

通用条例 第4条	除非法律另有规定，每个电子系统运营商都有义务运营符合以下最低要求的电子系统： A. 可根据法律法规规定的保留期重新显示电子信息和/或电子文件的全部; B. 在运营电子系统时，能够保护电子信息的可用性、完整性、真实性、保密性和可访问性; C. 能够按照电子系统实施的程序或说明运行; D. 提供语言、信息或符号可被电子系统运营方所理解的程序或说明;以及 E. 建立一个可持续的机制，以保持程序或指示的时效性、明确性和问责制。	华为云作为云服务提供商，提供云硬盘、对象存储等多种存储服务，客户可依据法律法规要求自行设定数据的保留期限。此外，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，充分利用云服务模式下按需使用、弹性扩展、可靠性高的特点，结合备份归档软件和华为云基础设施，将客户云下数据备份归档到华为云。 华为云保护租户数据的机密性、完整性、可访问性等方面的全面数据保护功能，并对相关功能的安全性负责。华为云绝不允许运维人员在未经授权的情况下访问租户数据。 华为云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。各可用区应有各自独立的UPS和现场备用发电设备，所有可用区域与多个一级传输供应商冗余相连，排除单点故障的风险。	客户（电子系统运营商）应按照法规要求保留日志记录，保证信息在系统中的可用性、完整性、机密性、真实性和可访问性、保证业务连续性，以印尼语提供服务使用说明，结合内外部法规要求的变化，将制度保持到最新。 为配合客户满足日志管理监管要求，华为云提供**云日志服务（Log Tank Service，简称LTS）**提供日志收集、实时查询、转储等功能，可长期保存日志。主机和云服务的日志数据上报至LTS后，存储时间可以在1-30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）、数据接入服务（DIS）中长期保存。 为配合客户满足保证数据机密性的要求，华为云提供服务端加密功能集成了**数据加密服务（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。DEW是一个综合的云上数据加密服务。它可以提供专属加密、密钥管理、密钥对管理等功能。其密钥由硬件安全模块（HSM）保护，并与许多华为云服务

			集成。用户也可以借此服务开发自己的加密应用。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，从而助力客户云上数据的安全。
电子系统注册 第6条	（1）每个电子系统运营商必须注册。 （2）在电子系统用户开始使用电子系统之前，电子系统运营商的注册义务已履行。 （3）电子系统运营商的注册应通过电子许可服务提交给部长，并根据法律法规的要求寻求电子集成。 （4）关于电子系统供应商注册的进一步规定，参考部级条例所规定的规范、标准、程序和准则。	华为云已完成向印尼当地部长提交注册所需的材料，进行私有范围电子系统运营者注册的工作。金融机构在注册账号后可以使用华为云服务。在使用云服务过程中，金融机构需遵从适用的法律和监管要求。	客户（电子系统运营商）应在用户开始使用系统之前，履行电子系统运营商的义务，遵循条例所规定的规范、标准、程序等。

硬件 第7条	（1）电子系统运营商使用的硬件必须： a. 满足安全、互联性和与所用系统的兼容性 b. 拥有卖方或供应商的技术支持、维护和/或售后服务;和 c. 保证服务的连续性。 （2）硬件须通过认证或其他材料来证明已满足要求。	华为云作为公有云服务提供商，所提供的云服务都是设计用于商业用途，采用的硬件具备互相兼容性。 云计算是一个复杂的IT软硬件及服务的组合，涉及到不同供应商提供的基础组件，而供应链的安全可信是整个云服务产品可信的重要组成部分。对于提供基础组件的供应链企业，华为云通过严格的供应商选择流程和绩效评估措施，确保产品和服务满足安全可信的需求。 华为云除了提供高可用基础设施、冗余数据备份、可用区灾备等外，还制定了业务连续性计划，并定期对其进行测试。该计划主要针对重大灾难，如地震或公共健康危机等，让云服务能够持续运行，保障客户的业务和数据安全。 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，华为云已获得众多国际和行业安全合规资质认证，全力保障客户部署业务的安全与合规。包括ISO27001、ISO20000、ISO22301等。	客户（电子系统运营商）应注意使用的硬件、软件必须满足安全、互联的要求，并能够保证业务的连续性。

软件 第8条	电子系统运营商使用的软件必须： a.保证运营的安全和可靠性;和 b.确保服务的可持续性。	交付安全可信的软件产品一直是华为公司倡导的企业文化。为了适应云环境下快速交付服务的需求，华为云在吸收业界先进理念的基础上，持续改进开发和运维流程，形成了开发、运维、安全一体化DevSecOps可信软件工程实践。华为云的DevSecOps可信软件工程实践通过工具和技术规范实现了流程的固化，使过程和结果透明可见、从故障现象到模块代码可追溯，从而实现云服务全生命周期的过程可信。 华为云秉承客户至上，服务第一的原则，根据基础级、开发者级、商业级、企业级不同级别的需求，建立可供选择的服务包，用户可通过在线工单、智能客服、自助服务、热线电话等多种方式获取专业的服务和帮助。任何用户均可通过多种渠道进行服务咨询、意见反馈和投诉建议，除基础性的站内在线客服和投诉建议热线电话外，系统复杂的企业客户可以选择适用的支持计划，获取由IM企业群、技术服务经理（TAM）、服务经理等组成的专属支持。	客户（电子系统运营商）应注意使用的硬件、软件必须满足安全、互联的要求，并能够保证业务的连续性。
电子系统治理 第11条	（1）电子系统运营商必须保证： a.服务水平协议的可用性； b.所用信息技术服务的信息安全协议的可用性；和 c.信息和内部通信设施的安全 （2）电子系统运营商必须确保整个电子系统的每个组件和集成都正常运行。	**《华为云服务等级协议》**约定了华为云各项产品/服务的服务等级，包括对服务可用性的承诺，以及未达到承诺的服务补偿。 华为云提供了线上的**《华为云用户协议》**约定了华为云的信息安全责任和保密义务。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（电子系统运营商）应根据服务水平协议、信息技术安全协议、内部通信设施的安全，确保电子系统可用性。

电子系统治理第12条	电子系统运营商必须对所造成的损害或损失实施风险管理。	华为云继承了华为公司的风险管理能力，建立了风险管理体系，并通过风险管理体系的持续运作，在复杂的内外部环境和巨大的不确定市场中实现有效的风险控制，力求业绩增长和风险之间的最优平衡，持续管理内外部风险，保障公司持续健康发展。 华为云在发生安全事件后，会对该事件进行风险评估，分析事件中的风险以及持续识别可能存在的新风险，对事件的风险进行控制。	客户（电子系统运营商）应实施风险管理。
电子系统治理第13条	电子系统运营商必须具备治理政策、操作程序和电子系统的审计机制。	华为云会对网络安全与隐私保护关系系统和关键数据进行风险评估，并配合审计要求对关键的信息系统和关键数据进行审计。	客户（电子系统运营商）应具备安全治理规划及工作程序，定期对电子系统进行审计。

电子系统治理 第19条	（1）电子系统运营商必须实施良好和负责任的电子系统治理。 （2）治理至少满足以下要求： a.电子系统运营中的程序或指令的可用性，这些程序或指令以各方理解的与电子系统运营相关的语言、信息或符号记录和/或公布； b.存在一个持续的机制来保持实施指南程序的新颖性和清晰性； c.电子系统正常运行的机构和支持人员是否齐全； d.对其运营的电子系统实施绩效管理，以确保电子系统正常运作；和 e.有计划保持其管理的电子系统运营的连续性。 （3）部委或机构可确定其他治理要求。	华为云作为云服务提供商，根据ISO27001标准，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。 华为云的产品或服务发布了操作说明书，且产品说明书有中英文版本，能够指导客户对产品或服务的使用并对操作说明书进行定期更新。	客户（电子系统运营商）应具备安全治理规划及工作程序，定期对电子系统进行审计。

电子系统治理 第21条	（1）私营范围电子系统运营商可以在印度尼西亚境内和/或境外对电子系统和电子数据进行管理、处理和/或存储。 （2）如果在印度尼西亚境外进行电子系统和电子数据管理、处理和/或存储，私营范围电子系统运营商必须确保该部委或机构和执法部门监督的有效性。 （3）私营范围电子系统运营商在监管执法范围内，依照法律法规的规定，应当提供电子系统和电子数据的访问权限。 （4）关于金融业私营电子系统运营商对电子系统和电子数据的管理、处理和存储的规定，由金融业监管部门进一步规范。	华为云会安排专人积极配合客户发起的审计要求。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。华为云已通过ISO27001、ISO27017、ISO27018、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。	客户（私营范围电子系统运营商）在监管执法范围内，应依照法规要求，保证执法部门的监督权力并提供电子系统和数据的访问权限。 金融客户（私营范围电子系统运营商）应遵循金融行业监管部门的规范。

电子系统运行安全 第22条	（1）电子系统运营商必须提供所有电子系统运营活动的审计跟踪记录。 （2）审计跟踪记录用于监督、执法、争议解决、核查、测试和其他检查的目的。	华为云的统一身份认证服务（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。当客户企业存在多用户协同操作资源时，使用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、访问控制列表来确保用户账户的安全。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（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。 华为云的运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。华为云还采用双因子认证对云为人员进行身份认证，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（电子系统运营商）应提供所有电子系统运营活动的审计记录，确保满足行为日志的留存要求，该审计记录会用于监督、执法、争议解决、验证等。 为配合客户满足日志管理监管要求，华为云提供**云日志服务（Log Tank Service，简称LTS）**提供日志收集、实时查询、转储等功能，可长期保存日志。主机和云服务的日志数据上报至LTS后，存储时间可以在1-30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）、数据接入服务（DIS）中长期保存。 为配合客户满足审计要求，华为云提供**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。 1. IAM提供适合企业级组织结构的用户账号管理服务，为企业用户分配不同的资源及 操作权限。用户通过使用访 问密钥获得基于IAM的认证 和鉴权后，以调用 API 的方式访问华为云资源。2. 如果租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，并访问租户的华为云资源。 3. 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。
电子系统运行安全 第24条	（1）电子系统运营商应拥有并执行保护电子系统的程序和方法，以避免中断、故障和损失。 （2）电子系统运营商应提供一个安全系统，其中包括用于预防和应对导致中断、故障和损失的威胁和攻击的程序和系统。 （3）如果由于另一方对电子系统的行为而导致系统故障或中断产生严重影响，电子系统运营商必须确保电子信息和/或电子文档的安全，并在第一时间立即报告执法人员和相关部委或机构。 （4）安全系统的进一步规定，由网络安全领域的政务机构负责人规定。	华为云建立了稳固、完善的边界和多层立体的安全防护系统。例如，多层防火墙对网络进行区域隔离；Anti-DDoS 快速发现和防护 DDoS 攻击；WAF 实时检测和防御Web 攻击；IDS/IPS 实时检测和阻断来自互联网的网络攻击、监控主机异常行为等。 鉴于安全事件处理的专业性、紧迫性和可回溯性，华为云拥有完善的安全日志管理要求、安全事件定级处置流程和7*24小时的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云秉承快速发现、快速定界、快速隔离与快速恢复的安全事件响应原则。同时，根据安全事件对整网、客户的危害刷新事件定级标准以及响应时限和解决时限等要求。	客户（电子系统运营商）应确保电子系统持续稳定运行，具备威胁对抗能力。如电子系统被入侵/故障导致产生严重影响，客户（电子系统运营商）必须确保系统内的信息安全，并在第一时间报告执法人员和相关部委/机构。 为配合客户满足日志管理监管要求，华为云提供**安全管理与态势感知分析平台（Situation Awareness，简称：SA）**，该平台能够检测出超过20大类的云上安全威胁，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。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，为用户呈现出全局安全态势。

电子系统运行安全 第25条	电子系统运营商必须按照法律规定确定的格式和保留期限重新显示完整的电子信息和/或电子文件。	华为作为云服务提供商，提供云硬盘、对象存储等多种存储服务，客户可依据法律法规要求自行设定数据的保留期限和格式。此外，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，充分利用云服务模式下按需使用、弹性扩展、可靠性高的特点，结合备份归档软件和华为云基础设施，将客户云下数据备份归档到华为云。	客户应确保电子系统运营商满足行为日志留存的要求以及其他安全要求。 为配合客户满足日志管理监管要求，华为云提供**云日志服务（Log Tank Service，简称LTS）**提供日志收集、实时查询、转储等功能，可长期保存日志。主机和云服务的日志数据上报至LTS后，存储时间可以在1-30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）、数据接入服务（DIS）中长期保存。

电子系统运行安全 第26条	（1）电子系统运营商应按照法律法规的规定，维护电子信息和/或电子文件的机密性、完整性、真实性、可访问性、可用性和可追溯性。 （2）在运营用于可传输的电子信息和/或电子文件的电子系统中，电子信息和/或电子文件必须是唯一的，并说明它们的控制权和所有权。	华为云对租户数据提供机密性、完整性、可用性、持久性、认证、授权、以及不可否认性等方面的全面数据保护功能，并对相关功能的安全性负责。但是，华为云只是租户数据托管者，租户对其数据拥有所有权和控制权。华为云绝不允许运维运营人员在未经授权的情况下访问租户数据。华为云关注内外部合规要求的变化，负责遵从华为云服务所必需的安全法律法规，开展所服务行业的安全标准评估，并且向租户分享我们的合规实践，保持应有的透明度。 华为云国际站《华为云隐私政策》中告知数据主体具有修改/更正或删除其被华为云收集的个人数据的权利，并提供了实现对应数据主体权利的途径（隐私邮箱和客服电话）。	客户（电子系统运营商）应依照法规要求，保证信息的机密性、完整性、真实性、可访问性、可用性和可追溯性。 为配合客户满足系统运行安全监管要求，华为云提供**统一身份认证服务（Identity and Access Management，简称：IAM）**提供适合企业级组织结构的用户账号管理服务，为企业用户分配不同的资源及操作权限。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。IAM 结合PAM功能还可以更有效地细化管理特权账户。
电子系统运行安全 第27条	电子系统运营商必须确保电子系统按照其设计的功能运行，同时仍考虑与以前的电子系统和/或相关电子系统的互操作性和兼容性。	华为云作为共有云服务提供商，所提供的云服务都是设计用于商业用途，并可与相关硬件、软件、互操作和兼容。 华为云作为共有云服务提供商，所提供的云服务都是设计用于商业用途，为保证服务的通用性和可移植性，采用了商业化的硬件、软件，以及常见、通用的技术格式和数据模式。	客户（电子系统运营商）应在保证系统按照业务逻辑运行的同时，确保电子系统之间的互操作性和兼容性。

电子系统运行安全 第28条	（1）电子系统运营商需要对电子系统用户进行教育。 （2）教育至少包括所有相关方的权利、义务和责任，以及提出申诉的程序。	在华为云官网中进行注册，为数据主体提供服务前，展示了用户协议和隐私政策，该政策能够被数据主体简单且清晰的获取和理解，并在注册界面告知数据主体需要对用户协议与隐私政策进行勾选同意才能为用户提供服务。 在隐私政策中说明和告知数据主体其享有的权利与义务和行使权利的方式，同意请求已电子方式明确提出。	客户（电子系统运营商）应对使用电子系统的用户展示相关方的权利、义务和责任，以及提出申诉的程序。
电子系统运行安全 第31条	电子系统运营商应保护其用户和更广泛的社区免受其运营的电子系统造成的损失。	为了加强网络安全防护，阻止网络攻击扩散，华为云参考ITU E.408安全区域的划分原则并结合业界网络安全的优秀实践，对华为云网络进行安全区域，网络层面的划分和隔离，使用了DDoS异常和超大流量清洗、网络入侵检测与拦截（IDS/IPS）、Web安全防护等技术手段。	客户（电子系统运营商）应增强安全防护能力，保护使用该系统的用户，避免他们利益受到损失。 为配合客户满足系统运行安全要求，华为云为客户提供基础设施，华为云将基础设施安全视为构筑多维全栈的云安全防护体系的核心组成部分。在物理环境、网络、平台、应用程序接口、数据等主要方面提供了多层次的安全防护，构建起多维立体、纵深防御和合规遵从的基础设施架构，用以支撑并不断完善涵盖了IaaS、PaaS和SaaS等具有优良安全功能的常用云服务。更多信息详见**《华为云安全白皮书》**中“7租户服务与租户安全”部分。

电子系统运行安全 第32条	（1）在电子系统运行环境中工作的每个人都有义务确保和保护通过电子系统传输的电子系统设施和基础设施或信息。 （2）电子系统运营商应提供、教育和培训负责电子系统设施和基础设施安全和保护的工作人员。	华为建立了完备的网络安全培训体系。在员工入职、在岗、晋升等环节纳入多种形式的安全技能培训，提升员工安全技能，确保员工有能力向客户交付安全、合规的产品、解决方案与服务。 a.网络安全基础培训：华为根据不同角色、岗位制定相应的安全基础能力培训计划。新员工转正前必须通过有关网络安全与隐私保护的上岗培训和考试；在岗员工需根据不同业务角色，选择相应课程进行学习与考试。管理者需参加网络安全必须的培训和研讨。 b.精准培训：通过大数据分析识别产品研发过程中的典型安全问题和问题关联责任人，并向其精准推送安全典型培训方案（包括案例、培训课程、练习题等），持续改进安全质量。	客户（电子系统运营商）应提供安全教育、培训等专项活动，提供员工信息安全防范意识和操作技能，保障公司和系统的信息安全。
电子系统运行安全 第33条	出于刑事司法程序的目的，电子系统运营商必须根据法律规定的权限，以及调查人员针对某些犯罪行为提出的合法请求，提供电子系统中包含的电子信息和/或电子数据或电子系统生成的电子信息和/或电子数据。	华为云应基于刑事司法程序的目的，根据法律法规和调查人员的合法请求提供相关数据。华为云提供**《华为云用户服务协议》**中约定“我们将采取适当的管理、物理和技术措施帮助您保护在服务环境下存储的您的内容的安全性和保密性。我们不会访问或者使用您的内容，除非是为您提供必要的服务，或者为遵守法律法规或政府机关的约束性命令”。	客户（电子系统运营商）应配合调查人员进行电子取证，提供某些犯罪行为信息/数据/系统衍生的信息/数据。
电子系统测试 第34条	（1）电子系统运营商需要进行电子系统性能测试。 （2）电子系统运营商根据保护需求的特点和电子系统运行的战略性质对电子系统中的所有组件或部分组件执行。	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 阶段的数据库安全等安全专项测试	客户（电子系统运营商）应对系统的性能进行测试。

义务 第39条	（1）在组织电子代理时，电子代理的组织者必须注意以下原则： a.谨慎; b.保障和整合信息技术系统; c.确保对电子交易活动的控制; d.成本效益和效率;和 e.根据法律规定保护消费者。 （2）电子代理运营商必须拥有并执行符合控制用户数据安全和电子交易原则的标准操作程序。 （3）控制用户数据和电子交易的安全性的原则包括： a.保密性; b.诚信; c.可用性; d.真实性; e.授权;和 f.免责声明。	华为云对租户数据提供机密性、完整性、真实性、持久性、认证、授权、以及免责声明等方面的全面数据保护功能，并对相关功能的安全性负责。华为云绝不允许运维人员在未经授权的情况下访问租户数据。华为云关注内外部合规要求的变化，负责遵从华为云服务所必需的安全法律法规，开展所服务行业的安全标准评估，并且向租户分享我们的合规实践，保持应有的透明度。 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。	客户（电子系统运营商）在使用电子代理时，应确保电子代理运营商具备并执行符合控制用户数据安全和电子交易原则的标准操作程序；且遵循电子交易的安全原则，包括保密性、诚信、可用性、真实性等。

6.2 电子代理运营商

	编号	具体控制要求	华为云的内部实践	客户的关注点

义务 义务 第40条	（1）电子代理运营商必须： a.进行身份真实性测试，并核实进行电子交易的电子系统用户的授权; b.制定并实施政策和程序，以在有迹象表明信息数据被盗迹象时采取行动; c.确保对电子交易系统、数据库和应用的授权和访问权限权的控制; d.编制并实施各种方法和程序，以保护和/或保密与电子交易有关的数据、记录和信息的完整性; e.拥有并实施对数据使用和访问的标准和控制，并在服务提供商有权访问数据时控制数据的使用和访问; f. 制定业务连续性计划，包括有效的应急计划，以确保电子交易系统和服务的持续可用;和 g.具有快速、适当地处理意外事件的程序，以减少电子系统事件、欺诈和故障的影响。 （2）电子代理运营商必须制定电子交易担保程序，以便客户不能被拒绝。	华为云作为数据处理者时，对云客户的数据内容不感知，且不会进行查看，仅按照云客户的指示开展个人数据相关的处理（存储、删除）。 华为云提供了IAM身份认证、DEW数据加密服务给客户来对个人数据进行保护防止未经授权或非法丢失、访问、使用、更改、更正或披露个人数据，同时通过IAM服务来对云客户进行认证鉴权。 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 阶段的数据库安全等安全专项测试。 鉴于安全事件处理的专业性、紧迫性和可回溯性，华为云拥有完善的安全日志管理要求、安全事件定级处置流程和7*24小时的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云秉承快速发现、快速定界、快速隔离与快速恢复的安全事件响应原则。同时，根据安全事件对整网、客户的危害刷新事件定级标准以及响应时限和解决时限等要求。 华为云除了提供高可用基础设施、冗余数据备份、可用区灾备等外，还制定了业务连续性计划，并定期对其进行测试。该计划主要针对重大灾难，如地震或公共健康危机等，让云服务能够持续运行，保障客户的业务和数据安全。	客户（电子系统运营商）在使用电子代理时，应 1.在系统安全方面，应核实电子系统、电子交易的用户授权、数据库的访问权限等，确保重要网络区域与其他网络区域之间采取可靠的技术隔离手段，防止未授权访问。 2.在管理制度层面，制定信息安全保护机制、信息安全事件应急响应计划、业务连续性计划等，保证能够快速高效的处理信息安全事件。

7 华为云如何遵从 2020 年第 5 号条例《关于私营电子系统供应商》及其修正案

通信和信息技术部在2020年11月24日发布第2020年5号条例《关于私营电子系统供应商》，规定私营电子系统运营商的注册，电子信息或电子文件的管理、审核，并要求断开私营电子系统运营商对禁用电子违禁信息或文件的访问。在2021年5月21日，通信和信息技术部发布了《关于私营电子系统供应商》的修正案。

以下内容将总结《关于私营电子系统供应商》中与云服务供应商相关的控制要求，并详细阐述了华为云的内部实践，以及华为云作为云服务提供商，如何帮助客户满足这些控制要求。

7.1 电子信息和/或电子文件的管理和审核

编号	具体控制要求	华为云的内部实践	客户的关注点

一般条例 第9条	（1）私营范围 PSE负责以可靠、安全和负责任的方式运行电子系统以及管理电子系统中的电子信息和/或电子文档。 （2）私营范围 PSE 必须根据法律规定以印度尼西亚语言提供服务使用说明。 （3）私营范围 PSE 必须确保： a.电子系统不包含任何禁止的电子信息和/或电子文件；和 b.电子系统不促进被禁止的电子信息和/或电子文件的传播。 （4）禁止电子信息和/或电子文件分类如下： a.违反法律法规规定的； b.扰乱社会和公共秩序；和 c.告知如何或提供访问被禁止的电子信息和/或电子文件的方法。 （5）扰乱社会和公共秩序指的是禁止使用的电子信息和/或电子文件，由该部委或机构根据法律法规的规定确定。 （6）不履行义务的私营范围 PSE 将根据本部条例的规定切断对其电子系统的访问（访问阻止）。	华为云在遵从所有适用的国家和地区的安全法规政策、国际网络安全和云安全标准，参考行业最佳实践的基础上，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、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放透明的方式，共同应对云安全挑战，全面满足云服务用户的安全需求。确保电子系统不包含、不传播任何违规的信息和/或文件。	客户（私营电子系统运营商）应安全稳定的运行电子系统，管理电子系统中的信息并根据法律规定以印尼语提供服务使用说明。同时，应确保电子系统不包含、不传播任何违规的信息和/或文件。 为配合客户满足电子信息的监管要求，华为云提供**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。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。需要强调的是，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。

私人电子系统运营商的义务 用户生成内容 第10条	（1）私营范围PSE用户生成内容必须： a.对电子信息和/或电子文件进行管理；和b.提供报告工具。 （2）电子信息/文件的管理至少应包含以下规定： a.电子系统用户使用电子系统服务的义务和权利； b. Private Scope PSE 在执行电子系统运营中的义务和权利； c.关于电子系统用户上传的电子信息和/或电子文件的责任的规定；和 d.设施和服务的可用性以及投诉的解决。 （3）报告工具必须可供公众访问，并用于提交对其管理的电子系统中包含的禁止电子信息和/或电子文件的投诉和/或报告。 （4）禁止电子信息和/或电子文件的投诉和/或报告，Private Scope PSE 应： a.向投诉和/或举报的人提供对投诉和/或举报的回应； b.对投诉和/或报告进行独立审查和/或要求对部长和/或相关部委或机构的投诉和/或报告进行核实； c.就电子系统用户上传的电子信息和/或电子文件的投诉和/或报告向电子系统用户提供通知；和 d.如果报告的电子信息和/或电子文件不是被禁止的电子信息和/或电子文件，则拒绝投诉和/或举报。 （5）未履行所述义务的私营范围 PSE 可以根据本部规的规定对其电子系	用户在使用华为云时，需要同意《华为云用户服务协议和隐私政策》。《华为云用户服务协议和隐私政策》中约定了华为云和用户义务和权利，用户在云上存储数据时的责任，以及华为云配合司法机构执法时提供用户数据。 同时，华为云平台提供工单系统作为提供公开投诉和/或报告的渠道，以用于用户对华为云服务或产品中包含禁止电子信息和/或电子文件的投诉或报告，运维人员对接反馈处理结果，以完成对这类投诉或报告的处理（包括向举报人回应、信息核实、用户通知、被禁止数据的访问/删除等）。	客户（私营电子系统运营商）应确保电子系统不包含、不传播任何违规的信息和/或文件。 客户（私营电子系统运营商）应对电子信息开展安全治理工作，制定安全规范，主要包括电子系统用户使用电子系统服务的义务和权利、私人电子系统运营商在进行电子系统运营的义务和权利、电子系统用户上传信息/文件的责任规定以及服务可用性、投诉问题解决等。 客户（私营电子系统运营商）应提供投诉路径，供用户投诉系统中存在的禁止信息/文件；并对投诉人反馈的问题进行核实和回应。

	统的访问（访问阻止）被切断。		
云计算运营商的义务 第12条	（1）云计算运营商必须对电子信息和/或电子文件进行管理。 （2）对于电子信息/文件的管理至少应包括以下内容： a.云计算服务用户使用云计算的义务和权利； b.云计算运营商开展云计算运营的义务和权利；和 c.关于云计算运营商服务用户在云计算上存储电子信息和/或电子文档的责任的规定。 （3）云计算运营商需要提供其控制下的云计算运营商服务用户的电子信息和/或电子数据，用于监督执法。	用户在使用华为云时，需要同意《华为云用户服务协议和隐私政策》。《华为云用户服务协议和隐私政策》中约定了华为云和用户义务和权利，用户在云上存储数据时的责任，以及华为云配合司法机构执法时提供用户数据。	客户（私营电子系统运营商-云计算运营商）应对电子信息和/或电子文件开展安全治理工作，包括云计算服务用户使用云计算的义务和权利；云计算运营商开展云计算运营的义务和权利； 和云计算运营商服务用户在云计算上存储电子信息和/或电子文档的责任的规定。 客户（私营电子系统运营商-云计算运营商）应配合监督执法，提供用户的信息/数据。

7.2 终止访问电子信息和/或禁用电子文件的申请

编号	具体控制要求	华为云的内部实践	客户的关注点
一般规定 第13条	（1）私人范围的 PSE 必须取消违规的电子信息和/或电子文件的访问权限。 （2）取消访问的权限包括终止对电子信息和/或电子文件的访问，以避免促进违规的电子信息和/或电子文件的传播。	华为云平台提供工单系统作为提供公开投诉和/或报告的渠道，以用于用户对华为云服务或产品中包含禁止电子信息和/或电子文件的投诉或报告，运维人员对接反馈处理结果，以完成对这类投诉或报告的处理（包括向举报人回应、信息核实、用户通知、被禁止数据的访问/删除等）。	客户（私营电子系统运营商）应及时取消违规电子信息/文件的访问权限，抑制违规信息的传播。

一般规定 第14条	（1）终止访问违规的电子信息和/或电子文件的申请可由以下人员提交： a. 公众； b. 部门或机构； c. 执法人员; 和/或 d. 司法。 （2）申请可以通过以下方式提交： a. 网站（网站）和/或应用程序； b. 非电子邮件； 和/或 c. 电子邮件（电子邮件）。 （3）提交违规内容的紧急申请，包括： a. 恐怖主义; b. 儿童色情制品； 或者 c. 扰乱公众、扰乱公共秩序的内容。	华为云平台提供工单系统作为提供公开投诉和/或报告的渠道，以用于用户对华为云服务或产品中包含禁止电子信息和/或电子文件的投诉或报告，运维人员对接反馈处理结果，以完成对这类投诉或报告的处理（包括向举报人回应、信息核实、用户通知、被禁止数据的访问/删除等）	客户（私营电子系统运营商）应关注公众、部门或机构、执法人员和司法机构可通过网站/应用程序、电子邮件等方式提交违规电子信息禁止访问的申请。

7.3 为监督和刑事执法目的提供电子系统和/或电子数据的访问权限

编号	具体控制要求	华为云的内部实践	客户的关注点
一般规定 第21条	（1）私营范围 PSE 有义务在监管范围内根据法律规定向部委或机构提供对电子系统和/或电子数据的访问权限。 （2）私营范围PSE 有义务在执法过程中根据法律规定向执法人员提供对电子系统和/或电子数据的访问权限。 （3）出于监督和执法目的而授予对电子系统和/或电子数据的访问权限的程序按照本部条例本章第二部分和第三部分的规定进行。	用户在使用华为云时，需要同意《华为云用户服务协议和隐私政策》。《华为云用户服务协议和隐私政策》中约定了华为云和用户义务和权利，用户在云上存储数据时的责任，以及华为云配合司法机构执法时提供用户数据。	客户（私营电子系统运营商）应在监管范围/执法过程中，根据法规规定向部委/机构、执法人员提供对电子系统/数据的访问权限。

为监控目的授予对电子系统和/或电子数据的访问权限的程序 第25条	（1）私营范围PSE必须指定至少一名居住在印度尼西亚境内的联系人，其任务是协助部委或机构提交的电子系统和/或电子数据的访问请求。 （2）联系人收到由部门或机构确定并提交给私营范围 PSE 的联系人的访问电子系统和/或电子数据的请求。	华为云在印度尼西亚境内有相关联系人，接收并以协助部委或机构（以监督或刑事执法为目的）提交的电子系统和/或电子数据的访问请求。	客户（私营电子系统运营商）应在指定至少一名居住在印度尼西亚境内的联系人，协助部委或机构提交的电子系统和/数据的访问请求。
为监控目的授予对电子系统和/或电子数据的访问权限的程序 第27条	自该部或机构的联系人提交请求后，私营范围 PSE 在不迟于 5（五）个日历日内完成第 26 条所述请求。	华为云在接收部委或机构、执法人员提交的电子系统和/或电子数据的访问请求（仅限于恐怖主义、儿童色情制品、贩卖人口、有组织犯罪、以及其他根据法律规定的对威胁生命和身体伤害的紧急情况）后，会进行点对点沟通，在5个日历日内完成相关请求。	客户（私营电子系统运营商）应在接到部委或机构联系人的请求后，在5个日历日内提供给部委或机构电子数据的访问。

为监控目的授予对电子系统和/或电子数据的访问权限的程序 第30条	（1）对 Private Scope PSE 提交的电子系统的访问是有限且保密的。 （2）部委或机构的官员才能使用该电子系统。 （3）授予对电子系统的访问权必须维护和保护： a. 电子数据的完整性、可用性和机密性； b. 电子系统的可靠性和安全性； 和 c. 在电子系统中存储、传输或处理的个人数据。	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、数据传输、数据存储、数据删除、物理销毁等方面，采用优秀的技术、实践和流程，为用户提供有效的数据保护能力，保障用户对其数据的隐私权、所有权和控制权不受侵犯。 在云服务中，我们讨论隐私保护的绝大部分场景是关于信息化的个人数据的处理，我们如何保护保障数据主体相关的权利以及如何保护个人数据的安全性。为此，华为云确定了个人数据处理的基本原则（合法正当透明、目的限制、数据最小化、准确性、存储期限最小化、完整性和保密性、可归责），并通过适当的管理和技术措施确保在处理个人数据时遵从基本原则。	客户（私营电子系统运营商）提供对部委或机构要求的电子系统的访问权限，应确保电子数据的完整性、可用性和机密性；电子系统的可靠性和安全性；维护在电子系统中存储、传输或处理个人数据的安全。
为监控目的授予对电子系统和/或电子数据的访问权限的程序 第31条	部委或机构的联系人提交请求后的 5（五）个日历日内由 Private Scope PSE 完成。	华为云在接收部委或机构、执法人员提交的电子系统和/或电子数据的访问请求（仅限于恐怖主义、儿童色情制品、贩卖人口、有组织犯罪、以及其他根据法律规定的对威胁生命和身体伤害的紧急情况）后，会进行点对点沟通，在5个日历日内完成相关请求。	客户（私营电子系统运营商）应在接到部委或机构联系人的请求后，私营电子系统运营商在5个日历日内提供给部委或机构电子数据的访问。

出于刑事执法的目的授予对电子系统和/或电子数据的访问权限 第37条	自执法机构联系人提交请求后，私营范围 PSE 在不迟于 5（五）个日历日内完成第 36 条所述请求。	华为云在接收部委或机构、执法人员提交的电子系统和/或电子数据的访问请求（仅限于恐怖主义、儿童色情制品、贩卖人口、有组织犯罪、以及其他根据法律规定的对威胁生命和身体伤害的紧急情况）后，会进行点对点沟通，在5个日历日内完成相关请求。	客户（私营电子系统运营商）应提供对执法人员要求的交通数据（交通数据）和电子系统用户信息（订户信息）的访问，在五个日历日内提供对执法人员请求的通信内容的访问。
出于刑事执法的目的授予对电子系统和/或电子数据的访问权限 第40条	（1）对 Private Scope PSE 提交的电子系统的访问是有限且保密的。 （2）电子系统的访问只能由执法机构使用。 （3）访问电子系统的请求必须维护和保护： a. 电子数据的完整性、可用性和机密性； b. 电子系统的可靠性和安全性； 和 c. 在电子系统中存储、传输或处理的个人数据。	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、数据传输、数据存储、数据删除、物理销毁等方面，采用优秀的技术、实践和流程，为用户提供有效的数据保护能力，保障用户对其数据的隐私权、所有权和控制权不受侵犯。 在云服务中，我们讨论隐私保护的绝大部分场景是关于信息化的个人数据的处理，我们如何保护保障数据主体相关的权利以及如何保护个人数据的安全性。为此，华为云确定了个人数据处理的基本原则（合法正当透明、目的限制、数据最小化、准确性、存储期限最小化、完整性和保密性、可归责），并通过适当的管理和技术措施确保在处理个人数据时遵从基本原则。	客户（私营电子系统运营商）提供对执法机构要求的电子系统的访问权限，应确保电子数据的完整性、可用性和机密性；电子系统的可靠性和安全性；维护在电子系统中存储、传输或处理个人数据的安全。

出于刑事执法的目的授予对电子系统和/或电子数据的访问权限 第41条	由私营范围 PSE 在不迟于执法机构联系人提交请求后的5（五）个日历日内完成。	华为云在接收部委或机构、执法人员提交的电子系统和/或电子数据的访问请求（仅限于恐怖主义、儿童色情制品、贩卖人口、有组织犯罪、以及其他根据法律规定的对威胁生命和身体伤害的紧急情况）后，会进行点对点沟通，在5个日历日内完成相关请求。	客户（私营电子系统运营商）应在接到部委或机构联系人的请求后，在5个日历日内提供给部委或机构电子数据的访问。
出于刑事执法的目的授予对电子系统和/或电子数据的访问权限 第42条	（1） 云计算运营商必须在执法范围内提供对电子系统和/或电子数据的访问权限。 （2）提供访问的义务仅用于与以下相关的紧急情况： a. 恐怖主义; b. 儿童色情制品； c. 贩卖人口（贩卖人口）； d. 有组织犯罪; 和/或 e. 根据法律规定，威胁生命和身体伤害的紧急情况。 （3）提供访问的义务应在自执法机构收到申请之日起五（五）个日历日内履行。	华为云在接收部委或机构、执法人员提交的电子系统和/或电子数据的访问请求（仅限于恐怖主义、儿童色情制品、贩卖人口、有组织犯罪、以及其他根据法律规定的对威胁生命和身体伤害的紧急情况）后，会进行点对点沟通，在5个日历日内完成相关请求。	客户（私营电子系统运营商）应根据法律规定，当发生紧急情况时（恐怖主义;儿童色情制品；贩卖人口（贩卖人口）；有组织犯罪; 和/或根据法律规定，威胁生命和身体伤害的紧急情况）向执法人员在五个日历日内提供对电子系统/数据的访问权限。

出于监督和刑事执法目的访问电子系统和/或电子数据的跟踪记录 第43条	（1）私营范围PSE 必须具有关于部委或机构使用电子系统访问权限的审计跟踪记录。 （2）私营范围PSE 可就各部委或机构使用电子系统访问权以下方面的影响进行评估： a.私营范围PSE向其电子系统用户提供的服务质量； b.保护其电子系统用户的个人数据；和/或 c.履行印度尼西亚法律法规规定的 私营范围PSE 义务。 （3）出于监督目的使用访问权限是在合理和负责任的期限内进行的。	华为云的统一身份认证服务（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。当客户企业存在多用户协同操作资源时，使用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、访问控制列表来确保用户账户的安全。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（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。 华为云的运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。华为云还采用双因子认证对云为人员进行身份认证，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。 华为云在为相关监管机构（部委或机构、执法人员）提供访问权限时，同样通过上述机构保存审计跟踪记录。	客户（私营电子系统运营商）应根据法律规定，当发生紧急情况时（恐怖主义;儿童色情制品；贩卖人口（贩卖人口）；有组织犯罪; 和/或根据法律规定，威胁生命和身体伤害的紧急情况）向执法人员在五个日历日内提供对电子系统/数据的访问权限。

出于监督和刑事执法目的访问电子系统和/或电子数据的跟踪记录 第44条	（1）私营范围的 PSE 必须有关于执法人员使用电子系统访问权限的审计跟踪记录。 （2）私营范围 PSE 可就执法人员使用电子系统访问权对以下方面的影响进行评估： a. Private Scope PSE 向其电子系统用户提供的服务质量； b. 保护其电子系统用户的个人数据； 和/或 c. 履行印度尼西亚法律法规规定的 Private Scope PSE 义务。 （3）出于执法目的使用访问权限是在合理和负责任的期限内进行的。	华为云的统一身份认证服务（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。当客户企业存在多用户协同操作资源时，使用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、访问控制列表来确保用户账户的安全。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（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。 华为云的运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。华为云还采用双因子认证对云为人员进行身份认证，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。 华为云在为相关监管机构（部委或机构、执法人员）提供访问权限时，同样通过上述机构保存审计跟踪记录。	客户（私营电子系统运营商）应具备执法人员使用电子系统访问权限的审计跟踪记录，访问权限应设定合理的期限。

8 华为云如何遵从 2007 年第 26 号条例《 关于互联网协议的电信网络使用安全 》及其修正案

通信和信息技术部在2007年5月4日发布了2007年26号条例《 关于互联网协议的电信网络使用安全 》，该法规主要针对使用互联网协议的电信运营商的要求。2017年1月24日, 通信和信息技术部发布了第2017年5号条例，对第2007年26号条例《 关于互联网协议的电信网络使用安全 》的修正案。

以下内容将总结《 关于互联网协议的电信网络使用安全 》中与云服务供应商相关的控制要求，并详细阐述了华为云的内部实践，以及华为云作为云服务提供商，如何帮助客户满足这些控制要求。

8.1 确保使用基于互联网协议的电信网络的义务

编号	具体控制要求	华为云的内部实践	客户的关注点

义务 第19条	（1）每个使用互联网协议的电信运营商都必须记录连接日志文件。 （2）连接记录至少保存三（三）个月。 （3）交易记录报告在线提交到数据库系统，用于监控和保护 ID-SIRTII 执行者拥有的基于互联网协议的电信网络的使用。 （4）如在线连接设施尚不可用，使用互联网协议的电信运营商必须每14（十四）个日历日以数字存储介质（存储介质）的形式向 LD-SIRTll 提交。	华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，日志包含资源ID（如：源IP、主机ID、用户ID等）、事件类型、日期时间、受影响的数据/组件/资源的ID（如目的IP、主机ID、服务ID等）、成功或失败等信息，以确保支撑网络安全事件回溯和合规。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。	客户（使用互联网协议的电信运营商）应确保业务日志至少留存三个月。 为配合客户满足日志管理监管要求，华为云提供**云日志服务（Log Tank Service，简称LTS）**具备日志收集、实时查询、转储等功能，可长期保存日志。主机和云服务的日志数据上报至LTS后，存储时间可以在1-30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）、数据接入服务（DIS）中长期保存。

义务 第21条	（1）网吧、热点等的管理者有义务在确保使用基于互联网协议的电信网络的情况下为每个互联网服务用户注册，至少包括： a.互联网服务用户的身份； b.使用互联网接入的开始和结束时间； （2）提供预付费服务的ISP 需要记录用户身份。 （3）互联网服务用户的身份数据必须至少保存1（一）年。 （4）就刑事司法程序而言，第（1）款和第（2）款所述的数据必须提交给主管当局。	用户需要在华为云官网注册方可使用华为云的服务，注册时需要提供必要的身份信息。在使用华为云服务期间，华为云会保存用户的账号信息。	公共热点的管理者应确保在用户注册后接入网络，需记录收集用户的身份，上网起始时间等信息。提供预付费服务的互联网服务提供商应记录用户身份。用户的身份数据至少保存1年。 为配合客户满足日志管理监管要求，华为云提供**云日志服务（Log Tank Service，简称LTS）**具备日志收集、实时查询、转储等功能，可长期保存日志。主机和云服务的日志数据上报至LTS后，存储时间可以在1-30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）、数据接入服务（DIS）中长期保存。
义务 第22条	（1）每个使用互联网协议的电信运营商都有义务按照总干事确定的服务器进行时钟同步。	华为云采用网络时间同步协议NTP（NetWork Time Protocol）使得通信设备与通信网的时钟时间同步，确保系统内各网元时间的一致性。	客户（使用互联网协议的电信运营商）应按照理事长的要求进行时钟同步，提供高精准度的时间校正。

9 结语

本文描述了华为云如何遵从法规与云服务供应商相关的控制要求，并详细阐述了华为云的内部实践，表明华为云遵从印度尼西亚通信和信息技术部（Kominfo）、印尼政府（Pemerintah Indonesia）、印尼法律和人权部（Ministry of Law and Human Rights）发布的重点监管要求，有助于客户详细了解华为云对印度尼西亚网络安全监管要求方面的符合性，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、构建和部署遵从印度尼西亚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。

本白皮书仅供一般性参考，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，并负责确保在使用华为云时对相关印度尼西亚监管要求的符合性。

10 历史版本

日期	版本	描述
2022年12月	1.0	首次发布