ICS 35.020
L 70

团　　体　　标　　准

T/BJCSA XXX-2024

算力网络安全指南

Guidelines for computing power network security

（征求意见稿）

2024-XX-XX 发布　　2024-XX-XX 实施

XXXXXXXXX　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由北京网络空间安全协会和广东省网络空间安全协会提出。

本文件由北京网络空间安全协会和广东省网络空间安全协会归口管理。

本文件起草单位：XXXX…。

本文件主要起草人：XXXX。

算力网络安全指南

1 范围

本文件提出了各类信息基础设施运营使用者采用算力网络的安全指引，给出了算力网络的生命周期各阶段应采用安全管理和技术措施。

本文件适用于指导各类信息基础设施运营使用者安全地采用算力网络，提供全生命周期的安全指南，适用于各类信息基础设施使用者采购和使用算力网络，也可供其他单位参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069-2022 信息安全技术 术语

3 术语和定义

下列术语和定义适用于本文件。

3.1

算力网络 computing power network

面向算网融合演进的新型网络架构，通过算力资源与网络资源状态的协同调度，将不同应用的业务通过最优路径，调度到最优的计算节点，实现用户体验最优的同时，保证用户体验和全局资源优化。

3.2

隐私计算 Privacy-preserving Computation

隐私计算是隐私保护计算的简称，它能够在保证数据提供方不泄露原始数据的前提下，对数据进行分析、处理和使用。包括联邦学习、多方安全计算、可信执行环境等。

4 算力网络概述

4.1 体制架构

4.1.1 概述

算力网络的体制架构应满足构建安全、高效、可扩展的算力服务的基础要求。该架构应分为三个主要层次：基础设施层、编排管理层和运营服务层，这三个层次应相互支撑，共同构成算力网络的核心框架。

4.1.2 基础设施层

基础设施层作为算力网络的物理基础，应包括各种计算资源、存储资源、网络资源以及相应的硬件和软件平台。这些资源应分布在不同的地理位置，通过各种网络连接形成一个统一的资源池。该层的安全性应重点保护物理设施免受自然灾害、人为破坏和网络攻击的影响，确保资源的可用性和完整性。

4.1.3 编排管理层

编排管理层应负责资源的统一管理和调度，通过智能化的算法和策略，根据应用的需求和网络的实时状态，动态地分配和释放资源。该层的安全性应关键保护管理系统的安全，防止未经授权的访问和恶意操作，确保资源调度的准确性和公正性。

4.1.4 运营服务层

运营服务层应作为算力网络与用户之间的接口，负责提供各种类型的算力服务，如云计算、边缘计算、人工智能计算等。它应通过友好的用户界面和丰富的应用程序接口（API），使用户能够方便地获取和使用算力资源。该层的安全性应重点保护用户数据的安全和隐私，防止数据泄露和滥用，确保服务的可靠性和合规性。

4.2 主要特征

4.2.1 概述

算力网络作为新一代信息技术的重要组成部分，应具备一系列鲜明的特征，这些特征定义算力网络的基本属性，并为其在各行各业中的广泛应用提供基础。

4.2.2 泛在连接性

算力网络应具备广泛的连接能力，能够覆盖从云端到边缘、从核心到末梢的各种计算节点。这种泛在连接性应使得算力资源可以像自来水或电力一样随时随地被用户所使用，极大地提高资源利用效率和用户体验。

4.2.3 智能调度性

算力网络应通过先进的算法和策略实现对计算、存储和网络资源的智能调度。这种智能调度性应根据应用的需求和网络的实时状态动态地分配和优化资源，确保各类应用的高效运行。

4.2.4 服务多样性

算力网络应提供多样化的服务类型。这种服务多样性应满足不同行业和用户的个性化需求，促进业务的创新和发展。

4.2.5 安全可信性

算力网络在设计和实现过程中应始终遵循安全可信的原则。它应采用先进的加密技术、身份认证和访问控制等手段确保数据和系统的安全。同时，算力网络还应具备强大的容错和恢复能力，确保服务的连续性和稳定性。

4.2.6 开放性和标准化

算力网络应作为一个开放的系统支持各种标准和技术的融合。这种开放性和标准化应促进算力网络的产业生态发展，使得不同的厂商和服务提供商可以共同参与到算力网络的建设和运营。

4.3 服务类别及业务场景

4.3.1 概述

算力网络的服务类别和业务场景应多样化，涵盖从基础计算到高级人工智能处理的各个方面，以满足不同行业和领域的业务需求。

4.3.2 服务类别

服务类别包括如下：

a) 基础计算服务。应提供标准的计算资源如CPU、GPU、内存和存储等，适用于需要弹性计算能力的各类应用场景如科学计算、数据分析等。
b) 存储与备份服务。应为用户提供持久化存储和数据备份能力，保证数据的安全性和可靠性，常见于企业数据备份、大型文件系统存储等场景。
c) 网络与传输服务。应负责数据在算力网络中的高效传输，提供低延迟、高带宽的网络连接服务作为实时通信、音视频处理等应用的基础。
d) 人工智能与机器学习服务。应为人工智能和机器学习应用提供专用的算力资源和算法库，支持模型的训练、推理和部署等服务。
e) 大数据与分析服务。应针对大数据处理和分析需求提供高性能计算和分布式存储能力以及相应的数据处理工具和算法帮助用户从海量数据中提取有价值的信息。
f) 行业定制服务。应针对金融、医疗、制造等特定行业的需求提供定制化的算力服务和解决方案以满足行业特定的安全、合规和性能要求。

4.3.3 业务场景

业务场景包括如下：

a) 自动驾驶。自动驾驶汽车需要大量的数据处理和实时决策能力，算力网络应提供强大的计算资源支持车辆的感知、定位和规划等功能。
b) 智能制造。在工业互联网场景下算力网络应能够实时分析生产线上的数据优化生产流程提高生产效率和质量。
c) 智慧城市。算力网络在智慧城市建设中应发挥重要作用支持交通管理、环境监测、能源管理等各类智能应用。
d) 金融科技。在金融领域算力网络应用于风险管理、交易系统、数据分析等方面提高金融服务的智能化水平和安全性。
e) 远程医疗。算力网络应支持高清视频会诊、医学影像分析、基因测序等医疗应用提升医疗服务的质量和效率。随着技术的进步和业务需求的增长算力网络的服务类别和业务场景将继续拓展和创新。

5 算力网络的安全风险

5.1 概述

根据算力网络的体制架构，算力网络安全风险主要可以归为技术风险、管理风险、应用风险和运营风险。

5.2 技术风险

技术风险包括如下：

a) 技术的不成熟与缺陷。在算力网络的发展和应用过程中，应认识到新技术可能伴随的不成熟性和缺陷。这些技术的不成熟和缺陷应被评估，以避免导致系统的不稳定、性能下降或安全漏洞。例如，引入新技术时，应评估其在实际应用中可能暴露的安全缺陷，并采取相应的预防措施。
b) 配置与管理的复杂性。在算力网络的配置和管理过程中，应考虑到涉及的计算、存储和网络资源的复杂性。应确保资源的配置和管理准确无误，以防止安全策略失效、访问控制不严或数据泄露等风险。同时，随着网络规模的扩大，应建立有效的管理机制，确保所有组件的安全配置和及时更新。
c) 兼容性与互操作性问题。在算力网络的设计和实施过程中，应重视不同厂商和技术的兼容性和互操作性问题。应确保硬件、软件或系统组件能够有效协同工作，避免因标准不统一、接口不
d) 兼容或协议不匹配等引发的安全漏洞或性能瓶颈。
e) 缺乏必要的安全防护措施。算力网络的安全防护应满足多层次、多手段的要求。在实际应用中，应避免因成本考虑、技术限制或管理疏忽等原因导致必要的安全防护措施缺失或不足。应建立全面的安全防护体系，包括有效的入侵检测与防御系统、充分的数据加密措施和完善的身份认证机制等。

5.3 管理风险

管理风险包括如下：

a) 管控复杂度提升。相较于传统网络架构，算力网络新型架构新增了网元，如算力网络感知单元和算力网络控制单元等，这些网元的引入将导致算力网络全网安全的管理复杂度提升，安全风险也随之增加。
b) 编排管理层汇聚风险。由于算力网络信息在编排管理层汇聚，算力信息的正确性、完整性、安全性将影响算力网络正常编排调度管理服务的开展。
c) 节点假冒风险。由于算力节点的多源泛在特性，一旦节点被攻击或仿冒，造成虚假算力信息上传，将严重影响算力网络的管理可靠性。
d) 数据管理风险。各类基础信息的大量集中存储，增加了黑客对编排管理层进行攻击，窃取或篡改数据的风险。一旦数据被窃取，可能会导致黑客对算力网络的非法利用，若数据被篡改，还会造成用户数据的泄露，影响运营服务的正常开展。

5.4 应用风险

应用风险包括如下：

a) 算力交易过程被攻击。在算力交易过程中，存在交易过程被劫持或中间人攻击的风险。算力交易数据存在被窃取或泄密的风险。算力交易的记录存在被删除、假冒、篡改的风险。
b) 算力并网引发安全问题。在各种类型算力接入网络的过程中存在利用接入身份验证机制的缺陷导致恶意算力接入引发算力网络崩溃的风险。除此之外在算力并网过程中，并网数据存在泄密、非授权访问、存储过程中篡改等风险。
c) 算力网络模型即服务安全风险。在应用模型即服务的过程中，对于服务模型可能进行非授权访问、数据输入干扰、输出结果被篡改和对API接口进行攻击的风险。

5.5 运营风险

运营风险包括如下：

a) 存证溯源困难。算力服务是端到端服务，用户群体庞大，分布式资源节点数量较多，数据信息管理起来较为繁杂，这导致存证溯源的复杂度提升，出现安全问题时难以快速定位安全威胁源。

b） 结果可信度。算力网络为多方算力节点提供算力对外输出的平台，可充分利用闲散算力资源，但存在引入不安全节点或恶意节点的可能性，影响计算结果可信度，攻击者或恶意节点还可能发起网络攻击或执行数据窃取等攻击行为，对服务稳定性、数据安全性等造成威胁。

c） 交易公正性。算力网络面向海量用户及节点提供算力交易服务，交易管理复杂，不诚实的交易参与方可能会篡改或否认交易结果，引发恶意计费、逃避计费等问题，影响算力交易的公平公正。

6 算力网络网络安全

6.1 算力网络安全框架

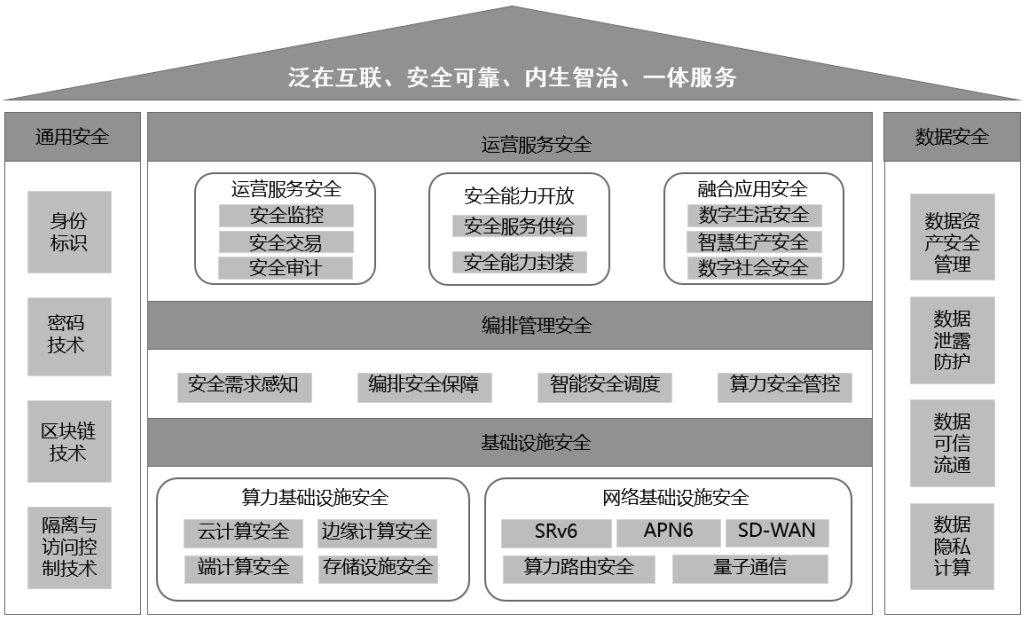

图1 算力网络安全框架

算力网络安全框架由通用安全、运营服务安全、编排管理安全、基础设施安全和数据安全组成，见图1。

a） 通用安全包括身份标识、密码技术、区块链技术、隔离与访问控制技术。

1） 身份标识。确保网络中每个实体（用户、设备等）都能够通过唯一的身份信息进行识别。

2） 密码技术。使用加密和解密技术来保护数据的安全性和完整性，防止未授权访问或数据泄露。

3） 区块链技术。基于区块链的去中心化和不可篡改的特性，为数据交换和存储提供安全保障。

4） 隔离与访问控制技术。通过物理或逻辑手段分隔不同的网络区域，实现细粒度的访问控制，以限制访问权限，防止未授权访问。

b） 运营服务安全包括运营服务安全、安全能力开放、融合应用安全。

1） 运营服务安全。确保算力网络的运营管理过程安全，包括设备的维护、软件的更新和补丁管理。

2） 安全能力开放。将安全服务和能力以API或其他形式开放给合作伙伴或开发者，促进安全

技术的共享和创新。

3） 融合应用安全。在算力网络中，多种应用和服务可能需要集成和协同工作，融合应用安全关注这些不同应用在集成时的安全性。

c） 编排管理安全包括安全需求感知、编排安全保障、智能安全调度、算力安全管控。

1） 安全需求感知。系统能够实时监控和识别安全威胁或需求的变化，并能够自适应地调整安全策略。

2） 编排安全保障。通过自动化工具和流程，协调各种安全措施和策略的实施，以提高安全管理的效率和效果。

3） 智能安全调度。基于人工智能和机器学习技术，自动化地识别威胁，分配安全资源，优化安全响应过程。

4） 算力安全管控。持续监控算力资源的使用情况和性能，以便及时发现并响应可能的安全事件。

d） 基础设施安全。

1） 算力基础设施安全。确保提供计算能力的硬件和软件资源免受攻击和滥用，保障算力供应的安全性。

2） 网络基础设施安全。保护网络设施和传输数据不受攻击，确保数据传输的安全和可靠性。

e） 数据安全。

1） 数据资产安全管理。涉及对数据资产进行分类、标识和保护，以防止数据资产的丢失、泄露或滥用。

2） 数据泄露防护。采取措施预防敏感数据外泄，包括监控数据流动、控制数据访问和实施数据加密。

3） 数据可信流通。确保数据在传输或交换过程中的安全性和可信度，使数据的使用方能够信任数据的来源和完整性。

4） 数据隐私计算。在处理个人或敏感数据时，采用技术手段保护数据隐私，如同态加密、安全多方计算等，以在不泄露数据内容的情况下进行数据处理和分析。

6.2 基础设施安全

6.2.1 概述

基础设施安全作为算力网络安全的基础，应满足硬件、软件和网络等多个层面的安全要求。在保障基础设施安全的过程中，需要着重考虑可信安全能力、安全加固能力以及稳定性安全保障能力等。

6.2.2 可信安全能力

算力网络可信安全能力应包括安全可信的计算环境、完善的安全加固能力和稳定性的安全保障能力。

基于可信根，算力网络各节点设备应在启动时对软件和固件进行可信验证，并在关键节点的应用程序的关键执行环节依据策略主动截获应用程序的系统行为（包括行为相关的主体、客体、操作等信息）对其进行可信验证，检测到其完整性被破坏后，采取相应安全措施，如停止启动、自动恢复、告警等。

算力网络的可信安全能力要求包括：

a） 算力网络设备应使用可信模块用于存储和管理加密密钥、测量平台状态并执行安全操作。采用可信的芯片，可以确保供应链侧不被植入后门。

b） 算力网络设备在硬件自举期间，可信固件应存储有关硬件完整性保护的哈希值，用于验证固件的完整性。

c） 基于可信模块，可信固件应验证加载的固件驱动及系统文件的完整性和来源是否合法。
d） 能够通过可信模块构建信任链，对固件、操作系统引导器和系统内核进行完整性度量。
e） 将测量者进行数字签名并发送给远程服务器验证，确保整个安全计算环境的安全性。算力网络的设备宜采用安全启动技术，确保只加载经过验证和授权的软件和固件。
f） 算力网络设备应采用安全更新机制，确保固件、操作系统、应用更新过程的安全性和更新内容的完整性。
g） 算力网络设备及服务宜采用多因素身份验证和细粒度的授权机制，确保合法用户的访问和操作。
h） 算力网络设备及服务应全面应用加密技术，并实施严格的密钥管理策略，保护数据安全。
i） 算力网络应确保基础设施供应链的安全，防止恶意软件或硬件被植入。

6.2.3 可信算力能力

可信算力的能力要求包括安全性能、可靠性能、可扩展性、兼容性、监管管理、维护和升级的容易性等 6 个方面：

a） 安全性能要求。算力网络应具备高度的安全性，包括防止未经授权的访问、防止数据泄露和保证数据的完整性等。
b） 可靠性能要求。算力网络应确保其提供的算力在可靠度方面是可信的，确保数据的准确性和完整性。
c） 可扩展性要求。算力网络应支持灵活地扩展算力资源，以适应需求的变化和扩展。
d） 兼容性要求。算力网络应兼容业界通用的算力平台与协议，以确保互操作性和通用性。
e） 监管管理要求。算力网络使用前需建立监管管理框架，确保系统或网络能够得到正确的监督和管理。
f） 维护和升级的容易性要求。算力网络应易于维护和升级算力的资源和平台，以便满足不断提高的可信算力需求。

6.2.4 安全加固能力

具体内容如下：

a） 基础设施具备合适安全基线扫描能力，包括：
——批量基线检查工具：具备批量导入数据功能，能识别并连接大规模基础设施。工具在大型资源池或 IoT 设备时可以降低工作量，提高工作效率；
——设备信息识别能力：根据设备提供的指纹信息，判断设备类型以及版本，由于不同设备的基线检查有较大区别，识别设备信息可以为基线检查工具提供合适的基线检查项；
——基线评分能力：检查设备基线后，根据基线的权重和引入风险的严重性，给予设备一定的评分，并且可以对所有基础设施提供总的评分等级，给出风险报告和改进建议。
b） 基础设施具备漏洞扫描能力，包括：
——检查网络中开放的端口、服务和协议；
——检查主机的操作系统及版本；
——通过已知漏洞的探测信息来探测主机/网络脆弱性；
——依据漏洞的严重性和漏洞的多少对基础设施进行漏洞/脆弱性评分；
——依据以上信息来判断基础设施存在的漏洞。
c） 基础设施根据基线扫描和漏洞扫描的结果，提供安全加固功能力，包括：
——利用工具，批量修复不合规的安全基线，如密码强度不够，防火墙配置为 any/any ，Root 用户可以远程访问等；
——利用补丁管理中心和批量漏洞修复工具，修复已知漏洞，例如更新第三方开源组件为新版

本，关闭不必要的服务/端口等；

——根据业界最佳实践实施安全配置（可选），例如关闭 log4j 访问端口 1389 和 4443 等重新对基础设施进行基线和漏洞评分，评分达到企业制定的标准时，可以停止本次安全加固。

d) 对算力网络各节点设备及所承载应用程序，参照设备及应用程序提供方提供的安全加固建议，结合实际应用场景进行安全加固，常见的加固项包括但不限于如下内容：

——禁用硬件设备的本地串口、本地调试口、USB 接口等本地维护端口；

——关闭不需要的系统和应用程序服务、默认共享、端口、不安全的访问协议；

——删除多余的系统和应用程序账号，并设置最小化访问权限；

——设置集群内防火墙策略，限制集群内部通讯端口的外部访问；

——启用复杂的口令策略、双因子认证等安全认证手段，并启用鉴别失败锁定防护功能；

——启用审计日志、异常告警功能；

——启用主机安全加固、入侵检测等安全防护设备，并使能防护策略及告警等。

e) 安全加固能力应对算力网络中的基础设施进行额外的安全防护和强化，具体要求包括：

——算力网络设备应实施严格的访问控制策略，确保只有授权的用户或系统才能访问和操作基础设施；

——算力网络设备应对敏感数据和通信进行加密处理，保护数据的机密性和完整性；

——算力网络运营商应建立漏洞管理制度，定期扫描和评估基础设施的漏洞，并及时修复；

——算力网络应部署入侵检测和防御系统，实时监控和分析网络流量和行为，及时发现并处置网络攻击。

6.2.5 稳定性安全保障能力

6.2.5.1 概述

网络稳定性安全保障能力主要指当网络面临不利条件、压力、攻击或妥协等网络安全事件时，具备以下能力：

a) 预测能力：保持一种对网络安全事件有充分准备状态的能力；

b) 承受能力：在网络安全事件发生后快速应急响应、吸收网络安全事件，在事件中生存下来，并持续运行关键业务的能力；

c) 恢复能力：在网络安全事件发生后快速恢复关键业务功能的能力；

d) 适应能力：系统具有修改业务功能或操作，以适应环境变化，不断提升抵抗风险的能力。

6.2.5.2 预测能力

预测能力指对网络安全事件有充分准备状态的能力，具有以下特征：

a) 可以识别关键业务、重要资产和服务，具备风险分析等明确的网络预测能力；

b) 具备检测/监测组件，可以识别对特定网络安全事件，并进行详细分析；

c) 检测/监测组件在算网系统中位于不同的物理位置和网络架构，并且故障时不影响正常业务使用。

6.2.5.3 承受能力

承受能力指遭受重大网络安全事件时系统关键业务的生存能力，具有以下特征：

a) 提高风险因素识别和补救措施的有效性，减少网络安全事件影响的时间和空间范围，降低网络安全事件由一个组织系统传递到另一个组织系统的感染和破坏能力；

b) 基于关键业务、资产和服务的优先级排序，对事件进行核实和评估，对故障进行快速有序地处理和恢复；

c） 持续提供基本业务功能、保证关键业务的生存底线。

6.2.5.4 恢复能力

恢复能力指在网络安全事件发生后快速恢复关键业务功能的能力，具有以下特征：

a） 明确备份的策略、需要备份的数据和文件内容、以及备份时间和备份方式。常见的备份策略有完全备份、增量备份、差异备份三种，备份数据或文件提供必要的安全保护，确保备份文件是干净的、可用的、没有被篡改或者破坏的；

b） 系统具备还原或回滚的功能，将备份数据恢复确保业务的运行；

c） 在网络中某功能节点失效后，可以采用其它具备相似功能的节点接替原失效节点的功能，实现节点接替。

6.2.5.5 适应能力

适应能力指为适应业务和环境变化，实现自适应地修改业务功能或操作的能力，具有以下特征：

——删除不安全的、不正确的或已经损坏的、可能造成损害的网络资源或数据，及时更新或修复失陷组件，降低网络安全事件发生的可能性。例如被植入的恶意代码或被指向恶意 URL 的 DNS 解析；

——提供威胁检测和阻断功能，阻止有可能发生的恶意活动采用重定向、动态隔离或者复杂加密手段等方式，延迟威胁到达目标的时间；

——采用冗余、替换等方式，快速实现系统重构，保持系统功能或性能水平。

算力网络所处物理环境应充分考虑环境规划、访问控制、电力电缆、消防、防水以及温湿度控制能力。

算力网络各节点设备应选用支持关键部件（如电源、风扇、硬盘、存储控制器等）冗余和热插拔设计、支持关键部件（如硬盘、内存等）故障隔离机制的产品，保证某一部件出现故障时，仍可提供基础服务。

算力网络关键节点应用应设置热冗余，对重要数据进行异地实时备份，并支持对重要数据进行本地备份及恢复功能。

稳定性安全保障能力应确保算力网络中的基础设施在面临各种异常情况和故障时仍能保持稳定运行。具体要求包括：

——算力网络宜通过冗余部署、负载均衡等手段提高基础设施的可用性；

——算力网络应建立完善的故障恢复机制，确保在发生故障时能够迅速恢复服务；

——算力网络应实施安全审计和日志分析制度，记录和分析基础设施的运行状态和异常情况；

——算力网络宜建立持续的安全监控体系，对基础设施进行实时监控和分析，确保及时发现并处置各种安全事件和威胁。

6.2.6 服务可访问控制

为了及时阻止未经许可的流量恶意注入算力网络，防止非法访问对算力服务造成的不利影响，应使用服务端对合法访问终端进行动态授权，并在数据转发层面对其业务流量进行合法性验证和无状态过滤，实现对算力网络和服务资源的有效防护。

——应全方位构建目标算力域鉴权授权机制，及时阻止无合法访问权限的、具有真实地址的算力终端非法访问业务行为；

——宜利用验证信息的统一化生成、一致性表达、动态更新管理以及轻量化抗重放机制，为算力业务访问提供高效的合法性验证依据，增强网络主动和被动抵御攻击的能力；建议在网络层

面进行近源、中间传输节点以及近目的的多点攻击防范，完善整套面向未来算网系统的攻击主动防范和溯源灵活阻断技术方案，达成流量实时高效检测控制的安全防护系统。

6.2.7 动态协同防护

为了提升资源利用率和业务处理效率，算网融合系统应要求安全防护机制随网络或算力资源调整进行动态适配与变更。

——应根据算力服务位置和算力网络状态的变化自动感应并调整安全策略，来保证安全防护的一致性与连续性；

——算力服务跨域部署或者迁移后，安全策略应进行相应的迁移和变更，以满足算力系统跨域防护要求；

——宜结合网元自身攻击防御能力、业务特征以及资源使用状况按需编排、设计安全传输通道，为多样化的算力应用个性化打造端到端算力业务防护面，构建高效业务传输和最优安全保障并存的算网防护体系。

6.3 网络通信安全

6.3.1 概述

网络通信安全作为算力网络安全的关键组成部分，应确保数据在传输过程中的保密性、完整性和可用性，通信过程中重要数据的机密性，网络边界访问控制信息的完整性，应采用身份鉴别、安全接入认证、密码服务和密码产品来保证网络通信安全。考虑到算力网络中数据传输的复杂性和多样性，以下方面应满足相应的安全要求。

6.3.2 接入安全能力

接入安全能力应保障算力网络中各类设备和终端的安全接入，特别是在跨城跨平面和多终端环境下。

a） 宜建立适应复杂网络环境的接入安全机制，采用强身份认证、加密通信和访问控制等手段，确保不同城市和平面间的安全接入。

b） 宜构建统一的终端安全管理平台，实施身份认证、安全策略管理和行为监控，以保障各类终端的安全接入和合规使用。

c） 应推动制定和完善安全接入协议及标准，促进不同厂商和设备间的互操作性和安全性。

d） 应针对不同组织和网络环境下的安全要求，采用身份鉴别、安全接入认证，密码服务和不同等级的密码产品，以保证网络的安全接入。

6.3.3 算力路由与协议安全

算力路由与协议安全应确保算力网络中数据传输路径的安全性和可靠性。

a） 宜确保算力路由算法的安全性和可靠性，采用加密和认证手段保护路由信息的传输安全，防止恶意节点对路由信息的篡改或欺骗。

b） 应确保算力网络中所用协议的安全性，及时修复和更新已知协议漏洞，并推动协议的安全标准化工作。

7 算力网络数据安全

7.1 数据流通安全

7.1.1 数据识别与分级分类

数据识别主要包括结构化数据、非结构化数据。根据数据的价值和重要程度划分，为不同级别的数据提供不同程度的安全防护。

——结构化数据识别应建立完善的敏感数据字段的识别规则和敏感数据特征，通过规则和特征匹配的方式识别出敏感数据字段，并进行校验和质量评估，最终输出敏感数据结果；

——非结构化数据识别宜采用基于相似度、非监督学习、监督学习等智能敏感数据识别技术，对文本、图像等数据类型进行智能识别与预测，并自动化输出数据类型结果。

算力网络中数据分级分类包括对交易信息、用户信息、节点信息等网络中收集存储的数据进行分级分类。

——数据分级分类应在遵循国家数据分类分级保护要求的基础上，一般根据业务属性将某领域内数据分为若干大类，再按照大类内部的数据隶属逻辑关系，将每个大类的数据分为若干层级，每个层级再分为若干子类；

——在数据分类基础上,根据数据重要程度以及泄露后对国家安全、社会秩序、企业经营管理和公众利益造成的影响和危害程度，对数据进行分级。数据分类分级应遵循科学实用、边界清晰、就高从严、点面结合、动态更新等原则。基于数据类别级别实施分级的安全保护，可以防止过度安全及安全措施的不足。

7.1.2 数据安全处理能力

算力网络中对于数据安全处理能力宜采用的安全措施包括：

——应具备高效且可靠的数据加密机制。在数据的传输和存储过程中，应采用国家商用密码加密算法，确保数据的机密性和完整性得到有效保护。同时，针对不同应用场景和数据特性，算力网络宜支持多样化的加密方式，以满足不同用户多样化的安全需求。

——应构建一套完善且严密的数据安全防护体系。包括但不限于使用多因素身份认证机制、精细化到字段粒度的数据访问控制策略、完善的数据安全审计制度等。

——宜注重数据治理和个人隐私保护能力的提升。在数据共享和交换的过程中，应建立健全的数据管理制度和个人隐私保护政策，确保数据的合规使用和隐私信息的有效保护。同时，算力网络还应加强对数据生命周期的管理，确保数据的合法性和安全性得到全程保障。

7.1.3 数据流转控制能力

算力网络中的数据流转主要分为：数据生产、数据流通和数据使用三个过程。

——在数据生产过程中，数据持有者应对数据资源拥有自主管控的权利，宜采取数据确权、存证审计相关技术。

——在数据流通过程中，应采取数据授权、匿名化、加密等相关技术。

——在数据使用过程中，宜通过隐私计算或机密计算为核心的技术构建密态数据流转互通网络，同时结合区块链等审计溯源技术，在管理面上实现数据安全可控。

在算力网络中，实现数据可控流转的核心就是保证数据加工使用权的跨域管控。

——使用权的跨域管控，指的是数据持有者在数据离开其控制域后，仍能对数据如何使用进行控制。具体方法为，首先通过合作协议，规定数据的应用场景、加工方式、使用次数、使用时间、结果获取等内容，实现“授权可管控”。

——在数据使用前，宜通过远程证明、代码审计等方式，实现“信任可验证”；在数据使用过程中，通过内存加密、内存隔离、密态存储、加密隧道等技术手段，实现“计算可隔离”。

7.2 隐私计算能力

7.2.1 基础能力

算力网络隐私计算基础能力宜包括：

a) 加密技术：包括对数据进行加密和解密的方法，确保数据在传输和存储过程中得到保护。常见的加密技术包括对称加密、非对称加密和哈希算法等。
b) 数据匿名化：通过对数据进行脱敏、扰动或匿名化处理，使得处理后的数据不再包含个人身份信息，从而保护用户隐私。
c) 差分隐私：一种隐私保护技术，通过向查询结果中添加噪音或干扰，使得查询结果不会泄露个体数据的隐私信息，同时尽可能保持查询结果的准确性。
d) 安全多方计算：多个参与者在不公开其私密输入的情况下进行计算，以确保计算过程中的数据保密性。
e) 可验证计算：确保计算结果的正确性和完整性，同时不泄露输入数据的详细信息。
f) 数据授权和访问控制：通过访问控制策略和权限管理机制，对数据的访问进行限制，只允许经过授权的用户或系统访问特定的数据。
g) 合规性与监管：确保数据处理和处理过程符合相关的法律法规和行业标准，同时提供审计和监管功能，以跟踪数据的使用和处理情况。

7.2.2 互联互通安全

算力网络隐私计算互联互通宜包括：

a) 身份认证和访问控制：采用身份认证机制和访问控制策略，确保只有经过授权的用户才能访问和处理数据，以防止未经授权的访问和数据泄露。
b) 数据脱敏：在数据交换和共享过程中，采用数据匿名化和脱敏技术，将个人身份信息和敏感数据转换成不可识别或不敏感的形式，以保护数据主体的隐私。
c) 安全计算协议：使用安全计算协议和隐私保护技术，如安全多方计算、同态加密、零知识证明等，实现在不共享原始数据的情况下进行计算和分析，确保数据隐私和安全。
d) 安全存储和访问控制：采用安全存储技术和访问控制策略，对数据进行加密存储和权限控制，限制数据的访问和操作权限，防止数据被未经授权的访问和篡改。
e) 法律和政策合规：遵守相关法律法规和隐私保护政策，制定和执行数据隐私和安全管理制度，保障数据处理和通信行为的合法性和合规性。

7.2.3 数据集安全对齐

不同数据提供方、数据集存在差异，在进行机器学习之前宜将各参与方的数据样本进行对齐：

——当数据集的特征空间重叠部分较大，样本重叠部分较小或没有重叠部分，在同一特征维度上进行样本熟练的扩充，应增加机器学习可用的数据量；
——当数据集的样本重叠部分较大，特征空间重叠部分较小或没有重叠部分，在同一样本空间上进行特征的扩充，应增加机器学习可用的特征维度。

7.2.4 特征工程

特征工程实现从多个数据提供方的多个数据集中，最大限度地提取特征以供机器学习，完成联合建模。

在特征工程阶段，多个数据方联合一起计算数据权重（WOE）和信息价值（IV）等，进一步确定联合建模的输入数据。

7.2.5 联合建模

联合建模应在任务发起方触发计算任务后，由算法方提供算法逻辑、数据方提供数据，在多方数据集上训练机器学习模型，由结果方获得训练好的模型参数和评估指标，包含：

——在多方数据集上实现机器学习模型训练，训练好的模型参数由结果方获得；

——结果方提供训练好的模型，计算评估指标判断模型训练的好坏，最终结果方获得评估指标结果。

隐私计算在联合建模过程中提供数据集中原始数据未经授权不应被除该数据提供方以外的其他方获知，计算结果应为各数据提供方的本地模式，各数据提供方应作为各自拥有其本地模型，中间迭代的本地模型参数明文及结果的本地模型参数明文不应被除各自结果方之外的各方所获知。

7.2.6 联合预测

联邦预测应由任务发起方触发计算任务后，数据方提供数据，由结果方获得预测的结果。其中数据包含预测的样本数据和模型数据。

隐私计算在联合预测过程中提供模型和待预测的样本数据，保证除了该数据提供方以外的其他方获知，并且预测的结果只有结果方能获得。

7.3 机密计算能力

7.3.1 概述

机密计算能力是算力网络安全的核心要素之一，用于保障数据在处理过程中的机密性、完整性和可用性。具体应满足以下要求。

7.3.2 基础能力

具体包括：

a) 应采用高强度的加密算法和密钥管理机制，确保数据在传输和存储过程中的机密性，并提供高效的解密机制，以满足授权用户的正常访问需求。
b) 应通过虚拟机、容器等安全隔离技术，实现不同用户数据和应用程序的隔离，防止数据泄露和非法访问，同时提供轻量级、可移植的安全运行环境。
c) 应采用内存加密、内存隔离等技术手段，保护计算过程中的内存数据，防止内存泄露和非法访问，确保内存数据的安全性和完整性。
d) 应建立安全审计和监控机制，实时监控和记录机密计算过程，及时发现和处理安全事件，确保数据的安全性和可用性。

7.3.3 互联互通安全

具体包括：

a) 应选择经过验证的安全协议（如 TLS、IPSec 等），保护不同节点之间的数据通信，确保数据在传输过程中的机密性和完整性，并对通信过程中的敏感数据进行加密处理。
b) 应建立严格的身份认证和访问控制机制，采用多因素身份认证、基于角色的访问控制等技术手段，确保只有授权用户才能访问机密计算资源。
c) 应建立跨域安全策略管理机制，统一管理和控制不同安全域之间的数据交互，通过策略配置、策略审核等手段确保数据交互的安全性和合规性。
d) 应建立安全事件处置和应急响应机制，及时处置和响应机密计算过程中发生的安全事件，提高安全事件处置和应急响应的能力和效率，并加强与相关方的协作和信息共享。

7.3.4 数据流动与共享安全

具体包括：

a) 应采用数据流动控制技术（如数据标签、数据脱敏等），确保数据在流动过程中不被非法获取或篡改，并建立数据流动审计机制进行实时监控和记录。
b) 应制定和实施共享安全策略，明确数据共享的范围、目的和权限等要求，通过数据加密、访问控制等技术手段确保共享数据的安全性和可用性，并建立共享数据的安全评估和审核机制进行定期检查和评估。

7.3.5 可信执行环境

具体包括：

a) 宜采用硬件和软件相结合的技术手段（如 TCM、TPCM、安全启动等），构建可信执行环境，确保计算环境在启动、运行和更新过程中的可信性。
b) 在分布式算力网络环境中，算力网络宜采用远程证明技术验证远程节点的身份和安全性，通过验证机制确保远程节点提供的机密计算服务符合安全要求。

7.3.6 机密计算节点

算力网络中安全任务（如机器学习模型）和敏感数据（如隐私数据）应该在机密计算节点上进行计算和处理，确保代码和数据在使用过程中的机密性与完整性，机密计算节点应提供如下能力：

a) 应采用安全硬件作为硬件信任根，安全硬件可包含 TPM、TCM、TPCM、CPU TEE、GPU TEE 等。
b) 应支持基于硬件信任根的可信引导与信任链构建，确保机密计算节点启动时的安全可信。
c) 应支持可信执行环境的动态创建，以机密虚拟机、机密容器、机密 enclave 等方式运行可信执行环境，无需重构代码即可支撑现有应用的运行。
d) 应支持可信执行环境的启动时完整性度量，确保可信执行环境启动时的镜像是符合预期的。
e) 应支持可信执行环境的内存加密，确保敏感数据不会通过内存被泄露。
f) 应支持可信执行环境的动态完整性监控，防止可信执行环境运行时被攻击。
g) 应支持可信执行环境的代码签名，确保只有合法的代码才能在可信执行环境内部运行。
h) 应支持封装存储功能，对敏感数据进行封装与加密保护，确保只有符合预期状态的可信执行环境才能解封数据。
i) 应支持可信执行环境的远程证明，确保可信第三方可以验证机密计算节点及其可信执行环境的身份与完整性状态。
j) 应支持可信执行环境的安全通信，确保可信第三方可以通过安全方式直接与可信执行环境交互。

7.3.7 机密计算服务

算力网络中应该提供机密计算服务，以支撑机密计算节点的安全构建，机密计算服务应包含：

a) 应提供注册服务，以支持对大规模异构机密计算节点的安全注册。
b) 应提供证明服务，以支持对大规模异构机密计算节点的远程证明。
c) 应提供完整性管理服务，以维护各种可信执行环境的完整性状态信息。
d) 应提供安全数据库服务，以安全存储机密计算节点以及可信执行环境的数据（如完整性值、注册信息、证明信息等）。
e) 应提供密钥管理服务，以支持大规模异构机密计算节点的密钥生成与管理。
f) 应提供证书管理服务，以支持大规模异构机密计算节点的证书生成与管理。
g) 应提供安全镜像管理服务，以支持机密虚拟机、机密容器、机密 enclave 等镜像的安全存储与管理。
h) 应提供代码签名验证服务，以支持大规模异构机密计算节点中工作负载的签名与验证。

i） 应提供可信计算服务，以为各种可信执行环境提供虚拟信任根与可信计算功能。
j） 应提供密码计算服务，以支持大规模异构机密计算节点的密码加速运算。

8 算力网络应用安全

8.1 算力交易平台应用安全

8.1.1 交易过程可信

具体包括：
a） 应保证交易活动全流程管控，确保交易数据不可篡改、交易过程可追溯，当发生交易争议等问题时，能够提供交易取证能力，进而实现交易过程全程可信的目标。
b） 可结合区块链技术对交易过程进行全流程标识化管理，将其中的关键环节或关键信息（订单信息、算网使用数据、计费信息等）上链存证，实现数据存证、数据防篡改功能。

8.1.2 权限管控

具体包括：
a） 应建立账号及用户权限管理机制，针对不同角色的用户，按照最小权限原则，合理分配操作权限（如增删改查等），以实现控制用户对特定资源的访问安全。涉及用户角色包括：算力网络需求方账号、算力提供方账号、算力应用提供方账号、平台运维人员账号以及管理员权限账号等。
b） 应通过限制接口接入设备、访问频次等方式对用户或系统接口进行管控。

8.1.3 交易风险评估

应具备对第三方算力资源、第三方算力应用、算力网络需求方的业务需求进行自动化风险评估的能力，具体包括对注册资质的自动化审核技术、篡改图片识别技术。

8.1.4 交易数据安全保护

具体包括：
a） 应对用户的个人信息进行保护，如对用户个人信息、企业资质材料等敏感信息进行加密保护处理；
b） 应使用数据加密技术保障交易数据的机密性，同时采取备份机制保证交易数据完整性和可用性；
c） 应采取安全传输技术保障用户与交易平台间、平台集群不同节点间以及运营服务平台与编排管理层间的数据传输安全。

8.1.5 交易安全审计

具体包括：
a） 应对平台日志进行管理，对用户登录操作、合约签订操作、平台报警与故障等情况进行日志记录，实现对交易过程的跟踪、管理，对报警、故障进行实时监控，进而实现交易流程和操作行为的可追溯性。其中，交易日志应至少包括以下信息：交易唯一标识、交易时间、算力提供方、服务需求方、业务需求、算力应用名称、交易算力信息标识、交易价格、交易模式、交易结果等；
b） 应提供审计接口，支持监管方或第三方审计机构访问交易日志、数据存证、电子服务合约等审

计资料，开展针对交易服务的安全审计工作；

c) 应只允许授权审计人员访问交易日志，实现对交易日志的查询和分析；

d) 应保证平台日志记录内容与安全审计结果的不可篡改、可追溯，并至少保存6个月以上。

8.2 算力并网安全

8.2.1 接入安全

具体包括：

a) 应对接入算力网络的三方算力提供者的用户和节点进行注册认证，应采取安全措施保证认证过程中及认证完成后节点身份信息的安全，防止信息泄露或被违规利用。

b) 算力节点入网前，应对节点的网络环境、网络边界防护能力、服务器环境、安全能力、可信度等进行安全测评，仅允许通过安全评估的算力节点加入网络。应至少满足GB/T22239-2019中第二级安全要求中7.1章节安全通用要求。

c) 节点接入算网后，应对节点安全状态进行监测，对于具有遭受网络攻击、行为异常等情况的节点及时进行处置。

8.2.2 数据安全

具体包括：

a) 应采用安全信道传输、数据加密传输等方式，保证数据在用户与算网之间、算网内不同节点之间数据传输的安全性。

b) 应建立数据流转安全保护机制，对于在不同提供者提供的节点间流转的数据，保障数据在前后节点的访问权限、安全策略一致。

c) 应建立数据流转追溯能力，采取技术措施对数据进行标记，一旦数据泄露，能够及时追溯泄露源头。

d) 在计算开展过程中，应建立数据访问控制、权限管理机制，对于多方数据共同参与计算的情况，对访问权限进行隔离，保障参与计算的用户只能访问到本方提供的数据。对于有高安全需求的业务，应保证计算过程中明文数据不在内存中出现，应采用机密计算、隐私计算等技术构建安全计算系统，满足业务安全需求。

e) 在数据存储过程中，应通过访问控制、权限管理等机制保证数据的访问安全。应通过加密等方法保证数据的内容安全。

8.2.3 网络安全

具体包括：

a) 应保证入网后的节点具备网络边界防护、入侵检测等网络安全防护能力，定期对节点开展远程安全运维，如基线检测、漏洞扫描等。

b) 对节点所处网络进行动态监控和定期审计，包括但不限于网络环境、网络安全防护能力变动等。

8.3 模型即服务安全

8.3.1 模型保护与授权管理

具体包括：

a) 对提供服务的模型进行版权保护和版本控制，防止未经授权的复制、修改和分发。

b) 应实施模型使用授权管理，确保只有经授权的用户和应用程序才能访问和使用模型服务。

c) 在提供模型即服务时需对模型的安全性进行全面评估，包括模型的数据隐私保护能力、抗攻击

性能、模型参数的保护等方面。

8.3.2 数据输入验证与抗干扰

具体包括：

a) 应对输入模型的服务请求进行严格的数据格式和内容验证，防止恶意输入导致模型失效或误判。
b) 宜采用对抗样本防御技术，增强模型对恶意干扰的抵抗能力。

8.3.3 输出结果审核与解释性

应对模型输出的结果进行必要的审核与确认，确保结果符合预期且无安全隐患。提高模型的可解释性。

8.3.4 服务接口安全与 API 管理

具体包括：

a) 应采用OAuth、JWT等标准对模型服务接口进行安全认证和授权。
b) 应对API进行版本管理和访问控制，防止未授权访问和滥用。
c) 应定期进行API安全审计，检查是否存在漏洞和安全风险。

8.3.5 服务可用性与连续性

具体包括：

a) 应保证模型服务的高可用性和业务连续性，可通过负载均衡、故障切换、冗余备份等手段确保服务稳定运行。
b) 应制定并执行服务级别协议（SLA），明确服务中断时的补偿措施，保护用户权益。

9 算力网络运营服务安全

9.1 概述

资源编排与调度安全在算力网络中至关重要，涉及网络资源和算力资源的合理配置与调度。为确保安全性，应满足以下要求。

9.2 资源编排与调度安全

9.2.1 概述

确保在算力网络、云计算环境或其他分布式计算环境中，资源编排与调度过程的安全性和可靠性。建立相应的安全机制和措施，确保在资源调度过程中，不会影响网络的安全运行和算力资源被恶意利用。

a) 实施访问控制和身份验证，防止未授权访问。
b) 保证调度算法的安全性，防止被恶意利用。
c) 实施网络安全措施，保护编排与调度过程中的通信。
d) 进行安全监控和审计，及时发现和响应安全事件。
e) 实现资源隔离，确保不同用户和应用程序之间的资源相互隔离。

9.2.2 网络维度安全

具体包括：

a) 应实施严格的网络隔离策略，划分不同的网络区域，如管理网、控制网和数据网，并限制区域间直接通信。同时，应采用访问控制列表（ACL）等技术手段，实现细粒度的网络资源访问控制。
b) 应部署网络流量监控系统，实时分析网络流量特征，检测异常流量和潜在攻击行为。利用大数据分析和机器学习技术，深度挖掘网络流量，以提前发现潜在安全威胁。
c) 应根据网络安全状态和业务需求，动态调整网络安全策略。例如，在检测到网络攻击时，应实时调整防火墙规则，以阻止恶意流量的传播。

9.2.3 算力维度安全

具体包括：

a) 宜实施算力资源隔离措施，通过虚拟化技术、容器化技术等手段，将不同用户的算力资源隔离开来，确保用户只能访问自己的资源。
b) 宜建立严格的算力资源访问控制机制，对用户进行身份认证和权限管理。只有经过认证且具有相应权限的用户才能访问和使用算力资源。
c) 应部署算力资源监控系统，实时监控算力资源的使用情况和性能状态。同时，应建立审计机制，记录用户对算力资源的访问和操作行为，以便进行事后分析和追溯。
d) 在制定资源编排与调度策略时，应充分考虑安全性因素。例如，应优先调度安全等级高的任务，避免将敏感数据暴露在不安全的计算环境中。同时，应定期对编排与调度策略进行安全评估和审查，确保其符合最新的安全标准和要求。

9.2.4 跨维度协同安全

具体包括：

a) 宜在网络和算力两个维度之间建立协同防御机制。例如，当网络层面检测到异常流量时，应触发算力层面的安全响应措施，如隔离异常算力节点、限制异常用户的访问权限等。
b) 宜建立统一的管理与调度平台，实现对网络资源和算力资源的集中管理、统一调度和协同防御。通过该平台，应能实时掌握网络和算力资源的安全状态和使用情况，及时发现和处理安全问题。

9.3 度量与标识信息安全

需考虑计费和资源协同等方面，通过建立相应的安全机制和措施，对算力资源和服务的使用情况进行准确的计量和标识，避免出现资源浪费或资源被恶意使用的情况。

a) 确保计费和资源协同过程中的信息安全性。
b) 使用加密技术保护度量数据和标识信息。
c) 实施严格的访问控制，确保只有授权用户能够访问计费和资源协同信息。
d) 定期进行安全审计，确保度量与标识信息的安全性。
e) 制定应急响应计划，以应对安全事件。

9.4 运营门户安全

在运营门户自身和用户操作等方面，要求保证门户的安全稳定运行，避免被黑客攻击或者恶意利用。

a) 建立资源访问和服务清单。
b) 实施强身份认证和访问控制机制，防止未授权访问。
c) 定期进行安全扫描和漏洞评估，确保门户的安全性。
d) 制定应急响应计划，以应对安全事件。

9.5 安全管理和监控

建立相应的安全管理体系和监控机制，对算力网络的运行状态和安全状况进行监控和分析，以便及时发现和处理安全事件。对算力网络中的资源访问和操作进行审计和监控，记录和分析日志信息，以便及时发现和处理安全事件。

9.6 安全合规和风险管理

遵守相关的安全标准和规定，对算力网络的安全风险进行评估和管理，以确保算力网络的安全运行和服务提供。

10 算力网络安全运营

10.1安全规范与策略

10.1.1 概述

安全规范与策略是确保算力网络安全运营运维持续有效管理的基础。具体应满足以下要求。

10.1.2 制定安全规范

具体包括：

a) 算力网络应明确访问算力资源的权限和审批流程，以满足防止未经授权访问的要求。
b) 算力网络应规定数据的存储、传输和处理标准，以满足数据机密性、完整性和可用性的保护要求。
c) 算力网络宜对算力设施的物理环境进行保护，以满足防止物理破坏和非法入侵的要求。
d) 算力网络应包括操作系统、数据库等系统的安全配置和管理要求，以满足系统安全性的保护要求。

10.1.3 制定安全策略

在安全规范的基础上，组织应制定具体的安全策略，以满足不同安全需求和场景的要求。这些策略应包括：

a) 应针对网络架构和通信制定安全策略，如防火墙规则、VPN配置等，以满足网络安全保护的要求。
b) 应针对应用程序制定安全策略，如输入验证、加密技术等，以满足应用程序安全性的保护要求。
c) 应明确在发生安全事件时的恢复流程和措施，以满足业务连续性的保障要求。

10.1.4 定期审查和更新

组织应建立定期审查机制，以满足安全规范与策略的持续有效性和适应性的要求。应定期审查和更新安全规范与策略，以确保其与技术发展和组织需求的变化保持一致。

10.2 安全运营人员要求

10.2.1 安全运营需求方人员要求

网络安全运营需求方人员是指对其所在单位的信息系统、基础设施、安全设备开展安全运营工作的人员。网络安全运营需求方人员需具备：

a) 了解网络安全运营组织架构，明确网络安全运营角色和职责；
b) 明确本单位网络安全运营的目标和方法；

c) 掌握既有网络情况，能够明确和评估业务系统面临的安全风险；
d) 根据应用系统特点和运行需求，充分与安全运营提供方人员沟通和协作，制定网络安全运营实施方案；
e) 能够识别与信息系统相关的所有资产，构建网络安全风险管理机制；
f) 定期监督、评估网络安全运营效果，确保网络安全运营符合业务需求。

10.2.2 安全运营提供方人员要求

安全运营提供方人员是指向运维需求方提供安全运营的人员。运维提供方人员需满足：

a) 为正式员工。需提供无犯罪记录证明，并通过安全背景审查，确保安全运营提供方人员安全可靠；
b) 根据不同的工作角色，安全运营提供方人员需具备下列技术和能力，包括但不限于：
   1) 针对物理环境、网络、系统的访问控制进行加固，以确保按照业务要求限制对信息和信息系统的访问；
   2) 基于信息安全策略，制定备份策略，保证备份的有效性和可靠性；
   3) 通过全面收集并管理信息系统及相关设备的运行日志，帮助排查定位和溯源网络安全攻击；
   4) 定期借助漏洞扫描工具对信息系统及其软硬件系统存在的漏洞进行扫描，发现存在的脆弱性，及时更新保持系统处于安全状态；
   5) 建立监视、发现、分析和报告信息安全事态和事件流程，确保快速、有效和有序地响应信息安全事件；
   6) 定期参与安全意识教育与培训，了解信息系统安全风险及安全运营责任及组织的信息安全策略和相关规程。
c) 每年完成不少于30个小时的网络安全意识或技能培训。

10.3 安全运营资源要求

10.3.1 概述

运营方应根据运行维护服务能力策划方案，按需建立和管理运行维护工具、服务台、服务数据、备件库、软件库和服务知识等支撑来自不同服务场景的服务需求实现，并与人员、过程和技术结合，保证资源能力满足价值实现过程中服务提供的需求。

10.3.2 安全运营平台

组织应在不同服务场景中使用工具支撑运行维护服务，以满足与需方约定的及需方未来的运行维护服务需求，促进服务价值的实现和创新。运行维护工具可分为监控工具、过程管理工具、专用工具，组织应通过工具提高服务效率和质量。至少应包括：

a) 依据服务需求，选择运行维护工具；
b) 制定运行维护工具的部署、应用方案并实施；
c) 必要时，通过技术研发实现工具间的集成；
d) 制定运行维护工具的管理制度；
e) 定期评估运行维护工具的应用效果并改进。

10.3.3 安全运营数据

组织应充分利用运行维护工具有效管理服务数据（如日志数据、威胁情报数据、监测数据、报告数据），以支持运行维护服务的量化管理或服务创新。至少应包括：

a） 针对服务场景的特点定义服务数据的类型、内容、格式等；
b） 制定服务数据的采集、存储、分析、处理、展示和利用等活动的管理要求；
c） 确保服务数据管理活动的合规性；
d） 利用工具对服务数据进行管理；
e） 制定服务数据质量管理和数据安全等方面的要求；
f） 对服务数据进行统计分析；
g） 运用服务数据分析结果，支持运行维护服务管理决策,改进运行维护服务的效率和质量。

10.3.4 安全运营知识

组织应充分利用运行维护工具和管理手段对服务知识进行全生命周期管理，以保证服务知识为组织的运行维护服务或创新提供支持，至少应包括：

a） 明确定义服务知识范围和类型；
b） 确定提炼并形成服务知识的管理要求；
c） 建立服务知识管理制度，管理知识的获取、评审、保存、分享等活动；
d） 使用适宜的技术手段实现知识的全生命周期管理；
e） 建立知识有效性及利用率的评价机制，以促进知识更新；
f） 宜通过应用知识建模、算法实现和特征工程等手段实现知识的深度学习和进化。

10.4 安全运营技术要求

组织应根据运行维护服务能力策划方案，实施技术研发和技术成果应用等活动，保证技术能力满足不同服务场景下的服务要求，实现其服务价值。

组织应根据策划对技术的要求进行技术研发，确保组织具备预防风险、发现问题、解决问题和优化创新的技术能力，至少应：

a） 确定技术研发范围；
b） 根据不同的服务场景，选择技术研发方式，方式包括自研、外采及合作研发等；
c） 识别和评估技术研发风险，采取有效控制措施；
d） 管理技术研发活动，监控和报告技术研发活动的执行情况；
e） 识别满足需求新技术机会，如包括基础设施运维技术、虚拟化技术、云计算技术、大数据技术、人工智能技术、SOAR、UEBA、AISecOps等；
f） 评价和验收技术研发成果。

10.5 应急响应与恢复

10.5.1 总则

根据 GB/T 24363-2009 的要求，结合算力网络的特点和实际需求，明确应急响应与恢复的要求，以指导和规范算力网络在面临安全事件时的应急响应与恢复工作，确保算力网络的安全稳定运行。

10.5.2 应急响应恢复组织

具体包括：

a） 建立专门的应急响应与恢复组织，明确组织结构和职责分工，确保在应急响应过程中能够迅速、有效地协调各方资源。
b） 定期组织应急响应与恢复演练，提高组织的应急响应能力和协作水平。

10.5.3 应急响应恢复计划

具体包括：

a) 制定详细的应急响应与恢复计划，明确应急响应的目标、原则、流程和措施，确保在发生安全事件时能够迅速启动应急响应机制。应急响应与恢复计划应包括如下几个方面：
   1） 算力资源调度与分配，算力网络应建立快速、动态的算力资源调度与分配机制，确保在应急情况下能够及时调整和优化算力资源分配，保障关键业务的连续性和稳定性。
   2） 云原生技术应急处理，针对算力网络中广泛应用的云原生技术，应建立相应的故障检测、隔离和恢复机制，确保在云原生组件出现问题时能够迅速定位并修复。
   3） 大规模数据处理与存储应急保障，算力网络涉及大规模数据的处理和存储，应制定数据备份、恢复和迁移等策略，并建立数据丢失或损坏时的快速恢复机制，确保数据的完整性和可用性。
   4） 多租户环境隔离与恢复，在算力网络的多租户环境下，应确保各租户之间的隔离性，并制定在不影响其他租户的前提下恢复故障租户服务的措施。
   5） 网络流量监控与调优，算力网络应建立网络流量监控和调优机制，实时监测网络流量状况，分析并解决可能出现的网络拥塞或故障问题，保障网络的稳定性和性能。
   6） 安全审计与日志分析，加强算力网络的安全审计和日志分析工作，记录关键操作和安全事件，以便在应急响应过程中快速获取关键信息，追踪攻击者轨迹，为应急决策提供有力支持。
   7） 协同与沟通机制，建立算力网络应急响应的协同与沟通机制，明确各部门和团队之间的职责划分、沟通渠道和协同方式，确保在应急情况下能够形成合力，高效响应和恢复。
b) 应急响应与恢复计划应建立事件分类分级识别机制，以满足及时发现并报告安全事件给相关人员的要求。
c) 应急响应与恢复计划应定期评估和更新，以适应网络环境和安全威胁的变化。

10.5.4 应急响应恢复流程

具体包括：

a) 应通过安全监控系统和安全日志分析等手段，实时监测网络的安全状况，及时发现并预警潜在的安全事件。
b) 应对发现的安全事件进行快速评估，确定事件的性质、影响范围和应急响应级别，并及时向上级主管部门报告。
c) 应根据安全事件的评估结果，迅速启动应急响应计划，采取必要的技术和管理措施，对安全事件进行处置，防止事件扩大和减少损失。
d) 应在应急响应处置完成后，及时恢复受损的系统和业务，并进行验证，确保系统的正常运行和业务的连续性。
e) 应建立定期的数据备份机制，以满足在发生安全事件时能够及时恢复数据的要求。
f) 应明确系统恢复的步骤和所需资源，以满足系统能够快速恢复正常运行的要求。
g) 应制定业务连续性计划，以满足在安全事件发生时保障业务连续性和可用性的要求。

10.5.5 应急响应恢复资源保障

具体包括：

a) 建立应急响应与恢复资源库，包括人员、设备、软件等，确保在应急响应过程中能够及时调配和使用所需的资源。
b) 定期组织应急响应与恢复资源的维护和更新，确保资源的可用性和有效性。

10.5.6 应急响应恢复培训与演练

具体包括：

a) 加强应急响应与恢复人员的培训，提高其应急响应能力和技术水平。

b) 定期组织应急响应与恢复演练，模拟真实的安全事件场景，检验应急响应计划的可行性和有效性。

11 算力网络服务的主要角色及安全责任要求

11.1 主要角色

即进行算力网络服务时涉及的实体角色，主要包括：算力网络提供方、算力网络需求方、算力应用提供方、算力网络交易服务提供方等。

注1：不同参与方可以由同一个实体担任。如：同一参与实体可能既是算力网络提供方，又是算力应用提供方。

11.2 安全要求

11.2.1 算力网络需求方安全责任要求

具体包括：

a) 算力网络需求方使用算力网络服务应具有明确、合理的目的，并按照双方协议约定的使用目的、范围、方式和期限使用算力网络服务；

b) 应保证业务需求的合规性，禁止处理和传播不良信息，禁止使用人工智能算法进行恶意的图片、音视频合成等操作。

11.2.2 算力网络提供方安全责任要求

应准确描述交易算力资源的来源、位置、大小等相关信息，并提供相关身份信息、资质材料、算力来源合法证明材料。

11.2.3 算力应用提供方安全责任要求

算力应用提供方应提供算力应用的算法逻辑、产品服务与特定场景需求相匹配，并提供说明材料。

11.2.4 算力网络交易服务提供方安全责任要求

具体包括：

a) 应取得我国行政或主管部门的经营认证许可资质；

b) 建立算力网络服务交易安全管理制度，包括但不限于：交易平台隐私政策、交易参与方信用管理制度和交易过程安全管理制度等；

c) 建立交易参与方的信用管理机制与奖惩机制。对多次违反交易安全要求、经常拖欠费用、不履约的参与方，可停止其交易权限，并对信用等级进行降级；对于评分较高、提供稳定算力资源的优质算力提供方，可对其信用等级进行升级；

d) 应定期对算力提供方提供的相关资质和算力来源合法性证明材料等进行审核，审核未通过的不应允许参与交易活动；

e) 应根据算力提供方的相关资质与信用等级、算力资源来源信息、用户评价等信息对算力资源进行动态风险评估，以确保交易算力资源符合国家相关法律法规的要求，并根据评估结果给出相应的算力资源安全等级认证标识；

f) 应定期对需求方的信用等级、相关资质等合法性证明材料声明进行审核，确保上述信息的及时

更新或处于有效期内，审核未通过的不应允许参与交易活动；

g） 应定期（如每年）或不定期对上述信用等级、评估结果、安全等级等进行动态更新。

参 考 文 献

[1] GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范