TC609

全国数据标准化技术委员会技术文件

TC609-6-2025-XX

全国一体化算力网 安全保护要求

National integrated computing network ——Security protection requirements

（征求意见稿）

2025 年 8 月 1 日

2025-XX-XX 发布　　2025-XX-XX 实施

全国数据标准化技术委员会　发布

目　　次

前　言

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。
本文件由全国数据标准化技术委员会（SAC/TC609）提出并归口。
本文件起草单位：

全国一体化算力网 安全保护要求

1 范围

本文件规定了全国一体化算力网的安全保护要求，包括通用安全要求、算力网资源安全要求、算力网调度安全要求、算力网监测平台安全要求、算力网运营安全要求和算力网数据安全要求等。

本文件适用于全国一体化算力网的安全能力建设、改造与优化。

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 25069—2022 信息安全技术 术语

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.2

算力 computing power,computility

图形处理器（GPU）、中央处理器（CPU）等设备执行计算密集型任务的计算能力。

3.3

算力资源 computing resources

计算资源、存储资源以及节点内部网络资源，通过该节点的管控系统/运营平台进行抽象并对外提供算力资源服务，或称算力资源节点。

3.4

算力网 computing network

支撑数字经济高质量发展的关键基础设施，可通过网络连接多源异构、海量泛在算力，实现资源高效调度、设施绿色低碳、算力灵活供给、服务智能随需

3.5

计算中心 computing center

或称为算力中心，为多用户提供计算服务的设施，可分为智算中心、超算中心、通算中心及混合算力中心等不同类型。用户的操作通过对计算设备及辅助硬件的操作及中心人员的服务实现。

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）
CPU：中央处理器（Central Processing Unit）
GPU：图形处理器（Graphics Processing Unit）

5 总体架构

全国一体化算力网安全框架以“安全可控、纵深防御、动态适应”为核心思想，通过六大安全维度要求，构建多层次、全方位、可持续的安全保障体系，确保全国一体化算力网在复杂多变的网络环境中，能够安全、稳定、高效的运行并提供服务。算力网安全框架（见图1）。

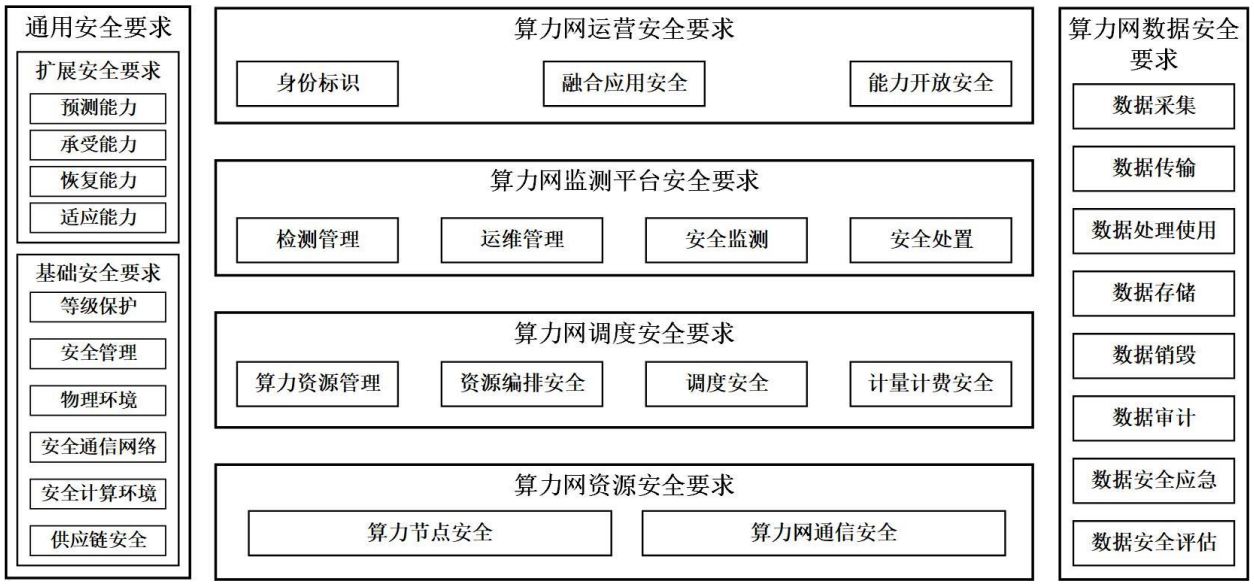

图1 算力网安全框架

a) 通用安全要求：主要包括基础安全要求和扩展安全要求。基础安全要求包括等级保护、安全管理、物理环境、安全通信网络、安全计算环境和供应链安全，确保算力网的基础架构具备坚实的安全保障；扩展安全要求涵盖了预测能力、承受能力、恢复能力和适应能力，以应对可能被高强度致命攻击、摧毁破坏等极端情况。

b) 算力网资源安全要求：聚焦算力基础设施本身的安全，确保构成算力网的“节点”与“连接”安全，具体包括算力节点（如计算中心、边缘节点等）的安全防护，以及算力网通信（节点间数据传输与协同）的安全保障。

c) 算力网调度安全要求：针对算力资源的高效、安全调度，提出算力资源管理安全、资源编排安全、调度过程安全以及计量计费安全的要求，确保资源分配科学高效、安全可靠。

d) 算力网监测平台安全要求：要求监测平台具备完善的安全管理功能、可靠的安全运维机制、实时的安全监控能力，以及高效的安全处置流程，实现对算力网安全状态的统一感知与应急处置。

e) 算力网运营安全要求：聚焦算力网日常运营过程中的安全风险，包括身份标识与访问控制（人员、设备、应用的可信身份管理）、融合应用安全（算力交易安全与审计）以及能力开放安全（运营门户、API 等对外开放服务的安全管控）。

f) 算力网数据安全要求：数据作为算力网的关键要素，要求覆盖数据全生命周期的安全保护，包括数据采集安全、数据传输安全、数据处理与使用安全、数据存储安全、数据销毁安全，并辅以数据审计机制、数据安全应急能力建设和常态化的数据安全评估，确保数据在算力网中流转和使用的全过程安全。

6 通用安全要求

6.1 基础安全要求

6.1.1 网络安全等级保护

a) 算力网及其部署在算力网内的应用系统应落实国家网络安全等级保护制度相关要求，开展网络和信息系统的定级、备案、安全建设整改和等级测评等工作；
b) 国家级、区域级或达到区域级规模的第三方监测调度平台，以及相关系统上线使用前应通过等级保护测评，保护等级不低于三级；
c) 算力资源层的智算中心、超算中心、通算中心、混合算力中心等，上线使用前宜通过等级保护测评；
d) 算力网发生重大变更或级别发生变化时，应重新进行等级保护定级备案与测评。

6.1.2 安全管理

6.1.2.1 安全管理制度

a) 制定算力网安全保护计划，明确网络安全保护工作的目标，根据本组织的安全风险排序，明确防护重点，指定或授权专门部门或人员负责网络安全保护计划、安全管理制度、操作规程等文档的制定，经审批后发布至相关人员，定期检查和更新网络安全计划，至少每年修订一次或发生重大变化时进行修订；
b) 基于本组织算力网面临的安全风险分析，制定安全策略，包括但不限于安全互联策略、安全审计策略、身份管理策略、入侵防范策略、数据安全防护策略、自动化机制策略（配置、漏洞、补丁、病毒库等）、供应链安全管理策略、安全运维策略等；
c) 基于算力网安全需求，建立安全管理制度体系，并形成管理制度文件和技术措施，包括但不限于风险管理制度、网络安全考核及监督问责制度、网络安全教育培训制度、人员管理制度、业务连续性管理及容灾备份制度、三同步制度（安全措施同步规划、同步建设和同步使用）、供应链安全管理制度等；
d) 根据算力网面临的安全风险和威胁，定期检查和更新网络安全保护计划、安全策略、安全管理制度等。

6.1.2.2 安全管理机构

a) 建立负责算力网的网络安全工作委员会或领导小组，由组织主要负责人担任其领导职务，明确一名领导班子成员作为首席网络安全官，专职管理或分管算力网安全保护工作；
b) 签发管理层文件，描述本组织网络安全管理机构职责、岗位、资源等，并定期对文件进行检查和更新；
c) 建立并实施网络安全考核及监督问责机制，明确网络安全考核目的、内容、方式等，以及网络安全问责对象、问责对象的责任界定和处罚措施等。

6.1.2.3 安全管理人员

a) 每年至少一次，对本组织网络安全管理机构的负责人和关键岗位的人员实施人员安全背景审查和安全技能考核，或在安全人员上岗前、身份背景发生变化、岗位发生重大变化的情况下开展背景审查，确保审查和考核通过方可从事相关岗位工作；
b) 应明确常规安全审查内容，如国籍、从业经历、教育背景、犯罪记录、个人信用、家庭情况等；
c) 应明确反间谍安全防范审查内容，如政治背景、海外关系等，通过访谈、调查等方式自行审查，或委托第三方调查机构审查；
d) 对审查资料进行归档留存，当本组织网络安全管理机构的负责人和关键岗位人员的身份、安全背景（如：取得非中国国籍、家庭情况）等发生变化时应及时更新，并根据情况重新按照相关要求进行安全背景审查。

6.1.3 物理环境

算力网及计算中心物理计算基础设施与环境，宜满足网络安全等级保护二级或更高级别的要求。

6.1.4 安全通信网络

6.1.4.1 网络架构

a) 应结合算力资源类型和资源情况，合理划分网络区域，制定网络拓扑与安全设计方案，并通过专家评审，在建设过程中严格按照设计方案实施项目，并定期更新网络拓扑；
b) 应实现通信线路“一主双备”的路由保护，宜对网络关键节点和重要设施实施“双节点”冗余备份；
c) 算力网各部分网络带宽和网络设备的处理能力应满足业务高峰期需要；
d) 网络边界和内部区域的网络、安全设备宜采用不同品牌异构部署。

6.1.4.2 互联安全

a) 应在不同的运营者之间、不同的计算中心、不同的安全区域之间、不同的计算资源之间、不同网络安全保护等级的系统之间、不同业务系统之间，建立或完善互联安全策略，包括数据交换、数据获取、数据流向、服务请求等相关的访问控制与边界防护等内容；
b) 应通过统一身份与授权管理系统对用户身份进行集中管理，保持同一用户身份、安全标记和访问控制策略等在互联的算力网络中一致性，包括用户安全标记、应用程序安全标记、业务数据安全标记等，以确保主体对客体访问控制策略的一致性；
c) 不同计算中心、安全区域之间的通信，应采用符合国家要求的密码技术为通讯传输提供保密性与完整性支撑；

6.1.4.3 边界防护

a) 应采取措施，对不同运营者、计算中心、安全保护等级系统、不同业务系统、不同区域之间的互操作、数据交换、信息流向进行严格控制；
b) 应制定信息流控制策略，控制不同的信息流动，包括限制受控信息流向互联网、限制重要数据流向境外、算力网信息系统或设备主动访问外部网络、限制跨区域数据流动、限制某些数据格式或含关键字的信息流出算力网；
c) 运营者应采取措施检测和管控未授权设备，只允许由运营者授权的软硬件运行。

6.1.4.4 安全审计

a) 明确审计范围，使用网络审计技术工具进行集中审计，监测并记录系统运行状态、日常操作、故障维护、远程运维等，存储相关日志数据不少于 6 个月；
b) 审计记录包括事件日期、时间、类型、主体标识、客体标识和结果等；
c) 保护审计记录，定期备份，避免未预期的删除、修改或覆盖等；
d) 保护审计进程，防止未经授权的中断；
e) 明确审查、分析、报告审计记录的策略，并定期进行更新；
f) 使用自动机制对审计记录进行审查和分析，监测和发现异常活动，并向相关人员或角色报告。

6.1.5 安全计算环境

6.1.5.1 鉴别与授权

a) 明确算力业务操作、重要用户操作或异常用户操作行为，并形成清单，内容包含操作说明、相关部门及岗位、业务流程、应用程序、安全防护措施等；
b) 在与设备、用户或其他服务或应用建立通信之前，对服务和应用程序进行标识与鉴别；
c) 在用户行为出现异常情况时应使用额外的鉴别机制实施身份鉴别，登录用户执行重要操作时应实施动态的或额外的身份鉴别；
d) 操作算力资源时，为主体、客体设置安全标记，并依据安全标记和强制访问控制策略确定主体对客体的访问。

6.1.5.2 入侵防范

a) 采用网络入侵检测、大数据分析检测等技术手段，防止高级可持续威胁（APT）等网络攻击行为；
b) 采用白名单、黑名单或其他方式，在网络出入口、算力业务系统中、实施恶意代码防护机制；
c) 增强算力资源系统的主动防护能力，实时监测与分析算力业务系统，及时识别并阻断入侵行为。

6.1.5.3 安全建设管理

a) 在新建或改建、扩建算力网时，应分析算力网的安全需求，明确算力网的安全要求，开展详细的网络安全设计，细化安全机制的具体实现；
b) 应在建设或改建、扩建算力网主体工程时，同步建设已规划的网络安全技术措施，建设完成后，将网络安全作为验收内容；
c) 同步运行网络安全技术措施，确保网络安全技术措施保持正常有效状态，与主体工程同时投入使用。

6.1.5.4 安全运维管理

a) 采用自动化方式管理、控制和审计运维活动，严格控制算力网远程运维的开通，确保算力网的运维地点位于中国境内，如确需境外运维，应按照国家相关规定执行；
b) 记录并保存运维日志，至少包括运维时间和活动描述、运维人员姓名、陪同人员姓名、被更新或替换的设备列表（如涉及设备维护）等信息。
c) 审核并监视运维工具的使用，如非必要尽量使用已在本组织登记备案的运维工具，如确需使用未登记备案的运维工具，在使用前应通过恶意代码检测等方式，确保维护工具未被不当修改。
d) 建立运维人员的授权流程和人员授权列表，定期审核更新运维人员授权列表，确保只有授权列表中的维护人员，才能进行系统维护，未在授权列表中的人员，必须在授权且技术可胜任的人员陪同与监管下，才可开展运维活动；

e） 对运维人员实施安全管理，签订安全保密协议，明确安全责任和义务。

6.1.6 供应链安全

6.1.6.1 供应链保护

应采取以下供应链保护措施，以降低攻击者利用供应链造成危害的可能：

a） 建立供应链安全管理策略，包括风险管理策略、供应方选择和管理策略、产品开发采购策略、安全维护策略等；

b） 建立供应链安全管理制度，提供用于供应链安全管理的资金、人员和权限等可用资源；

c） 优先购买现货产品，避免购买定制设备，如确需购买定制设备，应自行或委托第三方网络安全服务机构对定制开发的软件进行源代码安全检测，或由供应方提供第三方网络安全服务机构出具的代码安全检测报告；

d） 强化采购渠道管理，在能提供相同产品的多个不同供应商中做选择，保持采购的网络产品和服务来源的稳定或多样性，以防范供应商锁定风险；

e） 建立和维护合格供应商目录，防范出现因政治、外交、贸易等非技术因素导致产品和服务供应中断的风险；

f） 使用可信或可控的分发、交付和仓储手段，在运输或仓储过程中对信息系统组件进行防篡改包装，如采取防伪标签、安全封条、中性化包装，不体现包装物的信息，对包装物的封箱、开箱过程进行监督和记录，对封条使用和货柜安全操作建立指导性规程；

g） 采用向供应商屏蔽关键信息、匿名采购或委托采购等方式，保护供应链相关信息，以降低因信息汇聚或关联分析而获得供应链关键信息的可能性，包括用户身份、产品或服务的用途、供应商身份、供应商处理过程等；

h） 使用多个供应商提供的关键组件并储备足够的备用组件，明确供应商选择和退出的机制。

6.1.6.2 产品和服务采购与使用

a） 采购、使用的网络产品和服务（如网络安全产品、网络专用设备、社会化云服务、安全检测服务），应符合法律、行政法规的规定和相关国家标准的要求；

b） 列入《网络关键设备和网络安全专用产品目录》的设备和产品，确保其按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可采购；

c） 对于可能影响国家安全的网络产品和服务，确保其按照网络产品和服务安全审查有关法规的要求通过网络安全审查，不应采购审查未通过的网络产品和服务；

d） 发现使用的网络产品、服务存在安全缺陷、漏洞等风险时，及时采取措施消除风险隐患，涉及重大风险的应按规定向相关部门报告。

6.1.6.3 产品和服务供应商管理

a） 采购网络产品和服务时，与供应商签订安全保密协议、供应商协议、服务级别协议（SLA），明确其安全责任和义务：

b） 应优先选择能够具备优质条件的供应商，包括但不限于，符合法律法规和政策要求、企业运转过程和安全措施相对透明、对下级供应商的关键组件和服务安全提供了进一步的核查、提供详细完整的硬件组件清单和产地清单等：

c） 在签署合同前对供应商进行评估，包括但不限于，分析供应商对信息系统、组件和服务的设计、研发、生产、实施、验证、交付、支持过程；

d) 加强供应商安全管理，要求供应商签订协议，供应商不得非法获取用户数据、控制和操纵用户系统和设备，不得利用用户对产品的依赖性谋取不正当利益或者迫使用户更新换代；
e) 要求供应商对网络产品和服务研发、制造过程中涉及的技术专利、知识产权等，获得十年以上授权，或在网络产品和服务使用期内获得永久使用授权。

6.2 扩展安全要求

为保障“东数西算”国家工程核心算力枢纽持续运行及其重要数据不受破坏的核心目标，面对国家算力网可能被高强度致命攻击、摧毁破坏、安全防线攻破、一招致命等极端情况，采用极限生存安全理念，通过快速恢复和动态适应，缓解攻击、化解风险，即使局部业务不可用，依然确保算力网的持续稳定运行。

6.2.1 预测能力

6.2.1.1 分析识别

a) 应识别算力网中关键节点的资产信息，包括资产地址、类型、厂商、型号等信息，对算力资产数据进行统一管理，分析资产类别、资产重要性以及资产所支撑业务的重要性；
b) 应识别算力网中资产存在的漏洞及配置缺陷，明确漏洞的详细信息，包括供应商、名称、版本号等内容，全面掌握算力网中的真实漏洞情况；
c) 应识别算力网中软硬件产品的供应商、软件组件、开源组件、开源代码、源代码、知识产权等信息，并对供应信息进行管理，以支撑对供应产品的监测和预警。

6.2.1.2 运行监测

a) 应能获取算力网中各层级设备的运行状态，如 CPU、内存、磁盘的占用情况及网络吞吐信息和资产实际通信关系，设置运行信息基线，当设备运行状态发生变化时及时告警；
b) 对算力网的网络行为进行监测，识别和分析异常离线、异常流量等行为，防范潜在威胁。

6.2.1.3 安全监测

a) 对算力网中关键节点重要资产和服务的安全状态进行定期检测与实时监测；
b) 实时掌握算力网中各计算中心的网络安全态势，可及时发现或识别已经发生、正在发生或可能发生的网络安全事件及其影响，监测网络安全事件发生的可能性和影响范围等；
c) 持续监测攻击活动的频率以及类型，并对疑似攻击进行分析，可发现未知攻击行为。

6.2.1.4 分析监测

a) 可对算力网进行细粒度分析，包括流量分析、安全事件分析、设备安全状态分析等；
b) 收集和分析威胁情报，包括漏洞库、利用情报库、失陷标识、IP 地址、域名等，应当建立健全漏洞信息接收渠道并保持畅通，留存漏洞信息接收日志不少于 6 个月；
c) 对安全分析数据与收集到的威胁情报资料进行关联分析，识别数据间的相关性。

6.2.2 承受能力

6.2.2.1 应急响应

a) 结合算力网的特点，制定应急预案，并定期组织应急响应培训和模拟演练，提高团队的应急处理能力，并确保应急预案的有效性；
b) 快速识别可疑终端和用户，并进行冻结或下线，以减少未经授权的访问和潜在的数据泄露风险；

c) 建立协同机制，确保在安全事件发生期间，所有相关方能够及时接收到必要的信息和指示。

6.2.2.2 动态防护

a) 制定详细的访问控制策略，包括访问控制列表（ACL）、基于角色的访问控制（RBAC）、基于属性访问控制（ABAC）或其他适合组织业务需求的访问控制模型；
b) 实施持续的安全验证措施，对用户和设备的身份进行实时确认，确保只有经过授权的实体才能访问算力网资源；
c) 宜根据用户和设备的行为模式、安全态势变化以及其他相关因素，动态调整其访问权限，以降低安全风险。

6.2.2.3 损失限制

a) 将算力网划分为多个小的、相互隔离的区域，以限制安全事件在网络中的传播，并在应急预案中明确，一旦算力网的信息系统中断、受到损害或者发生故障时，需要维护的关键业务功能；
b) 具备最小化授权能力，控制不同人员的操作维护权限，加强设备操作管控；
c) 实时监控网络和系统的行为，及时发现异常活动并快速响应。

6.2.2.4 基线运行

a) 优先保障算力网中的关键业务，制定资源分配策略、业务连续性计划和应急响应流程，优先为关键业务分配必要的计算、存储、网络等资源，以保障关键业务的基本运行；
b) 设计和实施基线化运行模式，确保在安全事件发生时，能够快速切换到此模式以维持算力网关键业务的基本运行；
c) 实施实时监控和评估机制，持续监控算力网中控制类组件的运行状态，并在必要时调整资源分配和运行策略。

6.2.2.5 业务供应链安全

a) 针对算力网中的关键业务，制定包括与系统、系统组件或系统服务的研发、设计、制造、采购、交付、集成、运营和维护以及处置相关的供应链风险管理计划；
b) 确保采购算力网所需的关键设备在网络关键设备和网络安全专用产品目录中；
c) 对于算力网中关键业务依赖的重要设备或服务，采用多供应商服务方式，并预留足够的库存和备用设备来应对突发的重大网络安全事件。

6.2.3 恢复能力

6.2.3.1 冗余配置

a) 算力网中关键业务的网络实施冗余机制，包括硬件冗余、软件冗余、网络冗余、安全冗余；
b) 设置重要系统和数据库的冗余，保证组件发生损坏或失陷时，存在可利用的资源实现系统重构；
c) 定期执行算力网数据的异地备份工作，并确保备份数据的完整性和可用性。

6.2.3.2 业务恢复

a) 具备在算力网遭遇安全事件或故障后快速恢复和重建受影响系统的能力，包括数据恢复、系统重建和服务恢复；
b) 制定并维护关键业务连续性计划，包括关键业务的备份流程、备用系统的启动程序和应急操作步骤；

c) 根据算力网的业务需求和风险评估，制定业务连续性计划（BCP）和灾难恢复计划（DRP）以及详细的预防措施、应急响应和恢复步骤，确保在安全事件发生后能够迅速恢复关键业务和服务；

6.2.3.3 灾备恢复

a) 准备必要的资源，包括备用设备、备用网络和备用电源，在业务中断时，能够迅速切换到备份系统或备用流，以支持业务连续性计划的实施；
b) 基于算力网中系统或业务数据的重要性，提供异地备份功能，利用网络将重要业务数据实时备份至备份场地；
c) 建立并定期测试备用系统和数据备份策略，包括模拟故障和恢复流程，确保算力网在主系统受损时能够迅速恢复关键业务。

6.2.4 适应能力

6.2.4.1 自主管理

a) 对算力网中带病上线的业务提供漏洞保护和安全策略的更新，支持多种操作系统和版本的漏洞检测，对不同的终端进行漏洞的检测，针对发现的漏洞，采取漏洞防御、实体补丁、虚拟补丁、轻补丁等策略进行修复加固；
b) 宜强化算力网中各类资产对于安全威胁的自身免疫能力，实现安全免疫，采用应用程序白名单防护技术，对程序进行保护，阻断非法进程运行。

6.2.4.2 业务重构

a) 通过设置多重系统、单元或其他实现同一功能的算力设备来保证组件发生损坏或失陷时，存在可利用的资源实现系统重构；
b) 基于算力网业务需求的变化，动态调整所调用的网络资源，快速重组系统功能，保证关键业务功能稳定运行，提高网络弹性；
c) 基于算力网业务需求，对业务流程进行重新编排或协调处理，避免引发级联故障或整体服务中断。

6.2.4.3 节点适应

a) 自动识别受损组件或网络节点，并快速切换到未损坏的组件或节点，替换已经损坏的组件或节点；
b) 当发生组件损坏或失陷时，能够利用可用资源快速重组系统功能，保证算力网中关键业务功能稳定，提高网络韧性能力。

6.2.4.4 网络适应

a) 根据运行环境的变化和威胁环境的变化，改变机制的使用方式，管理如何使用机制。

7 算力网资源安全要求

7.1 算力节点安全

算力网算力节点应满足如下要求：
a) 应明确算力节点接入算力网的安全标准，并对其合规性进行评估；

b） 应对算力节点进行安全性、稳定性、兼容性进行评估；
c） 应支持节点认证，确保节点接入身份安全；
d） 应保障计算过程安全性；
e） 应支持节点隔离，如发现节点存在风险及时采取隔离措施。

7.2 算力网通信安全

算力网算力节点通信应满足如下要求：
a） 应明确算力节点接入算力网的通信标准，并对其合规性进行评估；
b） 应支持安全资源编排，算力网络通信流量按照规划的路径传输；
c） 应采用低延时安全设备，保障算力节点之间的网络传输时延；
d） 应保障算力节点间数据交换带宽；
e） 应对算力网不同算力节点之间通信进行流量规则检测、异常行为检测，及时发现报文篡改、漏洞攻击等攻击行为；
f） 应具备基于流量检测技术的内部流量机动检测能力，按需检测内部风险。

8 算力网调度安全要求

8.1 算力资源管理

a） 算力节点应通过身份认证和鉴权方式注册到算力网络平台，确保算力节点的合法性，防止非授权的算力节点接入算力网络；
b） 应对算力节点与算力平台注册消息中的设备标识、位置信息等关键信息进行隐私保护，防止隐私信息在发送过程中出现泄露；
c） 应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；
d） 应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；
e） 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。

8.2 资源编排安全

a） 算力资源编排策略，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；
b） 应对算力节点与算力平台之间通信启用保护机制，应支持提供传输层安全传输通道的 SSL/TLS 协议，保证算力节点与算力平台通信传输安全性，算力节点和算力平台之间的应使用端到端的加密和认证功能，保证数据的完整性和机密性保护；
c） 应支持算力节点的访问控制能力，算力平台可通过黑白名单机制对算力节点的通信接口实现访问控制，应支持对算力节点与算力平台通信报文的限制，防止算力节点的流量过载导致网络拥塞；
d） 应支持在算网平台上对算力节点的版本信息、安全环境信息、开启的服务及端口信息、权限信息等安全健康度信息的呈现，并支持对算力节点的版本远程升级、安全漏洞修复、服务的远程开启等安全的远程加固，对算力节点的访问记录审计；

e） 应支持对算力的证书管理，并通过安全的通道保证证书传输的机密性和完整性；
f） 应支持算网编排中的日志记录，包括算力节点的访问日志、编排管理的行为日志等，以及相关日志的审计。

8.3 调度安全

a） 应为算力节点赋予全网唯一安全标识，根据算力节点软硬件版本、安全配置，对其安全能力进行动态评估并能够进行安全等级划分，以及持续监控节点安全状态，异常时触发告警及响应机制；
b） 应实施用户注册鉴权以确保任务申请合法性，通过加密通道保障通信机密性与完整性，实时监控用户状态并动态调整权限，同时保护用户敏感数据以防止隐私泄露；
c） 应支持对计算任务的安全性评估，并根据其安全等级动态适配到相应安全能力的算力节点，满足安全调度的要求；
d） 应完整记录调度日志，定期开展安全审计。

8.4 计量计费安全

a） 应使用加密技术保护度量数据与标识信息，并确保计费与资源协同过程的信息安全；
b） 应实施严格访问控制，确保只有授权用户能够访问计费和资源协同信息；
c） 定期开展安全审计，保障度量与标识信息安全。

9 算力网监测平台安全要求

9.1 检测管理

a） 应遵守相关的安全标准和规定，对算力网络的安全风险进行检测和管理，以确保算力网络的安全运行和服务提供；
b） 应在算力节点加入算力网络后，对其进行安全检测，以及算力节点运行期间对算力节点相关系统的主机、应用、容器等的漏洞扫描和安全基线合规性核查，并及时进行安全整改；
c） 应提供对算力节点镜像的安全管理能力，支持镜像可信，镜像仓库源可信检测，支持镜像扫描和基线核查，并使用哈希算法对镜像完整性校验，对镜像权限和访问控制；
d） 应对算力节点的安全策略和配置的实施、变更等维护操作进行管理，防止因配置不当或误操作而导致的运营安全风险。

9.2 运维管理

a） 应支持算力网络平台对算力节点的配置策略、算力能力信息、操作维护和管理信息传输的机密性完整性保护；
b） 应支持算力节点信息的访问和操作启动授权保护，并遵循权限最小化原则，建立权限分离机制；防止非授权的篡改；
c） 应对算力网络管理人员和维护人员进行集中的身份认证管理与访问控制。包括集中账号管理、认证授权管理、访问控制和行为操作安全审计；
d） 应保存算力网络相关系统的登录、维护操作、安全等日志信息，并定期开展算力网运维相关日志的安全审计，包括但不限于账号和权限审计、异常行为审计等方面，审计记录留存。

9.3 安全监测

a) 应对算力网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；
b) 应采用安全日志管理和入侵检测等技术对算力交易进行实时安全监控，覆盖从用户开通算力资源到资源释放整个流程；
c) 应实时监测算力节点资源运行状况，及时发现和处置安全风险。

9.4 安全处置

a) 应对算力资源进行访问控制，确保只有授权用户和程序能够使用所辖算力资源；
b) 宜通过限制算力用量、拒绝算力请求或降低算力用户信用等措施对非法算力使能行为进行管控。

10 算力网运营安全要求

10.1 身份标识

a) 应对算力网络访问主体进行身份管理及访问控制，包括终端、用户、设备等，实现算力网络中用户、算网基础设施、上层应用等实体的全面身份化；
b) 应定义和管理每个访问主体的身份角色，明确身份权限管理要求。

10.2 融合应用安全

10.2.1 交易安全

a) 针对中心式算力交易场景，应依托第三方中心交易平台应制定统一的安全策略；
b) 针对分布式交易场景，应以区块链技术为主，在链节点上进行信息展示和交易流程，且所有链节点同步节点信息，实现分布式算力安全统一运营；
c) 算力交易过程中应确保交易参与方的真实可信、交易过程的安全可控，做到安全事件可追溯；
d) 交易过程可追溯，安全风险可防范。

10.2.2 安全审计

a) 应对算力交易流程进行识别、记录、归档整理以及分析，对于重要记录需进行备份，确保出现问题时有据可查；
b) 应对算力网络中重要数据（包括系统数据、配置参数、业务数据和用户数据等）访问行为进行记录和审计，追溯数据的各处理环节；
c) 可借助区块链的智能合约、多方共识等技术在算力网络中实现对行为的审计溯源，提升算力网络数据处理环节的公信力。

10.3 能力开放安全

10.3.1 运营门户安全

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

10.3.2 API 认证与鉴权

a) 开放能力封装后通过 API 的形式对内外提供服务，应对 API 请求的合法性进行认证，必要时进行双向证书认证；
b) 应根据用户分配指定的权限，对 API 请求行为进行权限检查，确认用户是否拥有访问该资源的权限；
c) 应确保用户访问 API 的认证与鉴权通过后才可访问算力网络资源的能力。

10.3.3 API 流量控制

a) 应使用负载均衡技术防止多个服务或应用大量的请求服务，导致超过服务的承受能力；
b) 算力网络运营平台可提供 API 流量控制能力， 根据业务需要提供一种或多种组合。

10.3.4 传输加密

a) 应使用链路加密等技术防止用户与算力网络服务间的通信数据在传输途径中被非法窃听导致信息泄露；
b) 应识别各种存在窃听风险的场景，提供端到端传输加密能力。

11 算力网数据安全要求

11.1 数据采集

算力网络数据安全在数据采集中应满足以下要求：
a) 应制定数据采集策略，并对采集策略的合规性进行评估；
b) 应明确数据采集源、采集方式、采集频率、数据分类分级、责任人等；
c) 应支持异构数据的实时采集；
d) 应支持对采集的数据进行格式转换，将同类型信息进行标准化；
e) 应支持对采集数据进行信息补充多类信息，如：资产信息、数据种类、所属业务等；
f) 应对数据采集过程采取必要的安全管控措施。

11.2 数据传输

算力网络数据安全在数据传输中应满足以下要求：
a) 应制定数据传输策略，并对数据传输合规性进行评估；
b) 应支持数据传输过程中的加密保护，采用密码算法符合密码管理要求；
c) 应支持传输数据的传输校验；
d) 应支持数据传输过程中状态、频率进行监控，并在出现异常时进行提示。

11.3 数据处理与使用

算力网络数据安全在数据处理与使用中应满足以下要求：
a) 应制定数据处理与使用策略，并对数据处理与使用合规性进行评估；
b) 应对数据使用和处理进行完整的审计，包括处理的主体、关键操作、操作时间的关键要素，支持对访问者身份进行溯源；
c) 应支持数据处理与使用的精细化授权管理；
d) 应支持数据处理与使用过程中的异常行为监控，并在出现异常时进行提示。

11.4 数据存储

算力网络数据安全在数据存储中应满足以下要求：

a) 应制定数据存储策略，并对数据存储合规性进行评估；
b) 应支持对敏感数据提供加密措施；
c) 应支持对用于调试、测试的敏感数据进行数据脱敏；
d) 应对数据存储建立冗余及备份机制；
e) 应支持数据存储的异常状态监控，并在出现异常时进行提示。

11.5 数据销毁

算力网络数据安全在数据销毁中应满足以下要求：

a) 应制定数据销毁策略，并对数据销毁合规性进行评估；
b) 应支持对已达存储期限无需保存数据、已完成服务目标不再使用数据、数据提供方要求销毁数据以及有关部门要求销毁的数据提供数据销毁；
c) 应提供多种数据销毁方式，如：删除法、格式化法、覆写法、粉碎法、消磁法等；
d) 应对数据销毁做好登记，并归档。

11.6 数据审计

算力网络数据安全在数据审计中应满足以下要求：

a) 应制定数据审计策略，并对数据审计合规性进行评估；
b) 应支持数据使用全程访问过程进行审计；
c) 应对审计、运维角色的运维操作行为进行操作行为审计，包括：增、删、改、查操作。

11.7 数据安全应急

算力网络数据安全在数据安全应急中应满足以下要求：

a) 应制定数据安全应急策略，并对其合规性进行评估；
b) 应建立安全监测体系，对算力网络、算力资源、数据、应用等实时监测，及时发现数据安全事件；
c) 应制定算力网络资源数据安全应急预案，明确应急响应流程和责任分工；
d) 应定期进行应急预案演练。

11.8 数据安全评估

算力网络数据安全在数据安全评估中应满足以下要求：

a) 应制定数据安全评估策略，并对其合规性进行评估；
b) 应具备对数据风险评估、检测的技术手段；
c) 应支持主动探测与被动发现方式识别在网数据资产，发现风险。