TC609

全国数据标准化技术委员会技术文件

TC609-6-2025-10

全国一体化算力网 安全保护要求

National integrated computing power network—Security protection requirements

2025-08-29 发布　　2025-08-29 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：公安部第一研究所、中国移动通信有限公司研究院、国家信息中心、国家数据发展研究院、中国电子技术标准化研究院、三六零数字安全科技集团有限公司、北京神州绿盟科技有限公司、天翼安全科技有限公司、杭州迪普科技股份有限公司、华为技术有限公司、北京天融信网络安全技术有限公司、深信服科技股份有限公司、江苏省未来网络创新研究院、深圳供电局有限公司、上海观安信息技术股份有限公司、江苏工程职业技术学院、安徽工程大学、兴唐通信科技有限公司、北京市大数据中心、海南州数据局、江苏博云科技股份有限公司、京东科技信息技术有限公司、新华三技术有限公司、浙江警官职业学院、中移（苏州）软件技术有限公司、江西省大数据中心、视联动力信息技术股份有限公司。

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。

本文件适用于全国一体化算力网的安全能力规划、建设、运营、改造与评估。

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

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

对网络环境下存储、传输和处理的信息的保密性、完整性和可用性的保持。

3.2

算力 computing power

综合数据处理能力，从处理能力的分类可划分为通算算力、智算算力、超算算力、量子算力等。

3.3

算力资源 computing power resources

计算资源、存储资源以及节点内部网络资源等集合，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。

3.4

算力网 computing power 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）

NPU：神经网络处理器（Neural network Processing Unit）

5 安全总体框架

全国一体化算力网安全框架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。全国一体化算力网安全框架见图1。

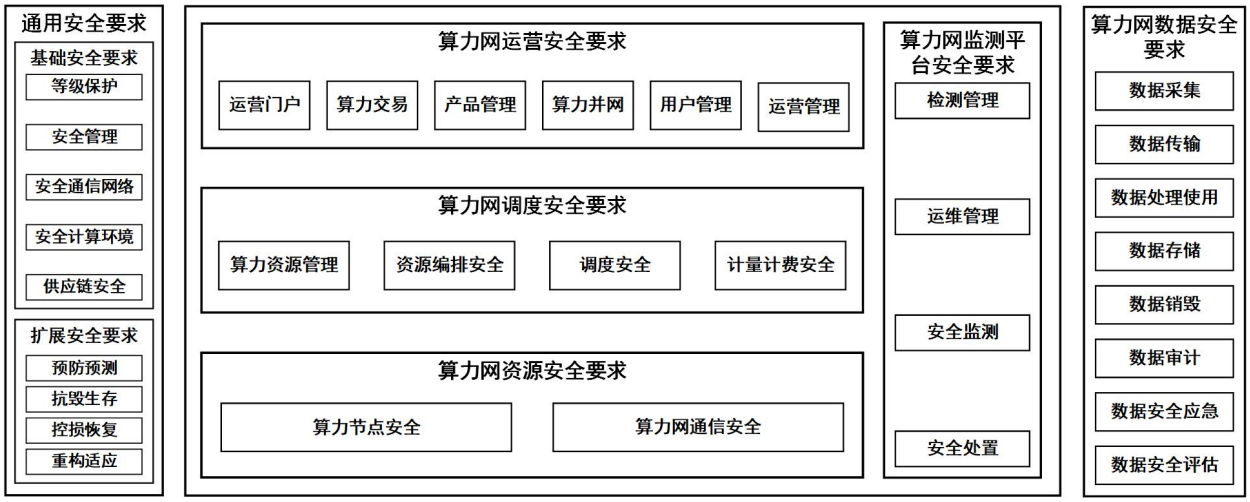

图 1 全国一体化算力网安全框架

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；扩展安全要求适用于避免风险级联效应导致重大或极端网络安全事件，包括预防预测、抗毁生存、控损恢复和重构适应能力；

b) 算力网资源安全要求：包括算力节点、算力网通信的安全要求；

c) 算力网调度安全要求：包括算力资源管理安全、资源编排安全、调度过程安全以及计量计费安全的要求；

d) 算力网监测平台安全要求：包括检测管理、运维管理、安全监测和安全处置的安全要求；

e) 算力网运营安全要求：包括运营门户安全、算力交易安全、产品管理安全、算力并网安全、用户管理安全和运营管理安全；

f) 算力网数据安全要求：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、数据审计安全、数据安全应急和数据安全评估要求。

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、等级测评和复审等工作；
b) 算力网监测调度平台、计算中心上线使用前应通过等级保护测评，保护等级不低于三级；
c) 国家级、区域级或达到区域级规模的算力节点，应按照 GB/T 39204 要求，开展安全能力建设；
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) 应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保护计划，至少每年修订一次或发生重大变化时进行修订；
b) 应制定安全策略，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、供应链安全管理策略、安全运维策略等；
c) 应建立安全管理制度体系，形成管理制度文件，包括但不限于网络安全考核及监督问责制度、安全风险管理制度、业务连续性管理及容灾备份制度、供应链安全管理制度、网络安全教育培训制度等，并定期检查和更新。

6.1.2.2 安全管理机构

a) 应成立算力网安全工作委员会或领导小组，设置算力网专门的网络安全管理机构，并签发管理层文件，描述本组织网络安全管理机构职责、岗位、资源等，定期对文件进行检查和更新；
b) 应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) 应对组织网络安全管理机构的负责人和关键岗位的人员，每年至少开展一次安全背景审查和安全技能考核；
b) 应在安全人员上岗前、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和技能考核，通过后方可从事相关岗位工作；
c) 应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、安全背景等发生变化时应及时更新。

6.1.2.4 安全建设管理

a) 在新建、改建或扩建算力网时，应分析明确算力网的安全要求，开展网络安全设计，细化安全机制；
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) 应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。

6.1.2.5 安全运维管理

a) 应管理、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) 应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等信息；

c) 应审核并监视运维工具的使用，优先使用已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，确保运维工具未被修改；

d) 应建立运维人员授权列表并定期审核更新，确保只有授权列表中的人员，才能进行系统维护，未在授权列表中的人员，必须在授权人员陪同与监管下开展运维活动；

e) 应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。

6.1.3 安全通信网络

6.1.3.1 网络架构

a) 应结合算力资源类型和情况，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) 开展攻击路径识别与威胁建模，并通过安全架构设计确保攻击路径关键节点得到充分的安全保护；

c) 算力网各部分网络带宽、网络设备和安全设备的处理能力应满足业务高峰期需要。

6.1.3.2 互联安全

a) 应在不同的计算中心、不同的安全区域、不同的计算资源、不同网络安全保护等级的系统以及不同业务系统之间，建立互联安全策略，包括数据交换、服务请求、资源隔离等；

b) 应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。

6.1.3.3 边界防护

a) 应对不同安全保护等级系统、不同业务系统、不同区域之间的互操作、数据交换进行严格控制，不同安全保护等级系统之间的互联边界，应满足较高安全保护等级系统的安全防护要求，限制从高安全保护等级系统向低安全保护等级系统数据流动，限制重要数据流向互联网、境外，限制设备、系统主动访问外部网络等；

b) 应在设备、软件接入前对其进行安全评估，并实时注册管理，实时监测设备接入，只有经授权的设备才能连接到信息系统，及时发现和阻止未授权设备接入并报警。

6.1.3.4 安全审计

a) 应明确审计范围，监测并记录系统运行状态、业务接口调用、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) 审计记录应包括事件日期、时间、类型、主体标识、客体标识和事件结果等；

c) 应采取措施保护审计过程，防止未经授权的中断；

d) 应采取措施保护审计记录，定期备份，避免未预期的删除、修改或覆盖等；

e) 应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。

6.1.4 安全计算环境

6.1.4.1 鉴别与授权

a) 应明确算力网业务操作、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) 设备、用户、服务和应用在建立通信前，应进行标识与鉴别；

c) 应为主体、客体设置明确的安全标记，依据安全标记制定访问控制策略。

6.1.4.2 入侵防范

a) 应采用入侵检测、大数据分析检测等技术手段，防止高级持续性威胁、挖矿、勒索、模型注入和诱导等网络攻击行为；

b) 应实时监测与分析系统行为，使算力资源系统具备主动防护能力，及时识别并阻断入侵行为。

6.1.5 供应链安全

6.1.5.1 供应链保护

a) 采购非标准化软件或设备，应自行或委托第三方网络安全服务机构，开展软件源代码安全检测，并出具检测报告；

b) 应强化采购渠道管理，在提供相同类型产品的多个供应商中做选择，保持采购网络产品和服务来源的稳定或多样性；

c) 应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；

d) 应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，对包装物的封箱、开箱过程进行监督和记录；

e) 应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。

6.1.5.2 产品和服务采购与使用

a) 采购、使用的网络产品和服务，应符合法律、行政法规的规定和相关国家标准的要求；

b) 应优先采购列入《网络关键设备和网络安全专用产品目录》的设备和产品，如需采购目录外的产品，应由具备资格的机构认证；

c) 对于可能影响国家安全的网络产品和服务，应通过网络安全审查，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，应及时采取安全措施，涉及重大风险的应按规定向相关部门报告。

6.1.5.3 产品和服务供应商管理

a) 采购网络产品和服务时，应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、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等；

c) 在签署合同前应对供应商进行评估，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) 应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) 应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。

6.1.6 密码要求

a) 算力网及部署在算力网内的应用系统，应确保使用的密码产品和服务满足国家商用密码要求；
b) 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信传输提供保密性与完整性支撑。

6.2 扩展安全要求

6.2.1 预防预测

6.2.1.1 风险识别

a) 应识别算力网中关键节点的资产信息，对算力网资产进行统一管理，分析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、知识产权等信息，并对供应信息进行管理；
d) 应对于经检测存在安全风险的业务提供安全隔离，支持多种操作系统和版本的漏洞检测，建立漏洞修复时效性指标并持续监控。

6.2.1.2 运行监测

a) 应获取算力网中设备的运行状态，如 CPU、GPU、NPU、内存、磁盘的占用情况及网络吞吐量等，当设备运行状态异常时及时告警；
b) 应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。

6.2.1.3 威胁分析

a) 应收集和分析威胁情报，包括漏洞信息、失陷标识、IP 地址、域名，以及威胁主体画像、算力行业威胁事件等；
b) 应建立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) 应对安全分析数据与收集到的威胁情报资料进行关联分析，识别相关性。

6.2.1.4 趋势预测

a) 应对算力网中关键节点的重要资产和服务，进行安全状态实时监测；
b) 应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，发现未知攻击行为；
c) 应实时掌握算力网中各计算中心的安全趋势，及时发现或识别已经发生、正在发生或可能发生的安全事件及其影响范围。

6.2.2 抗毁生存

6.2.2.1 应急响应

a) 应制定应急预案，定期组织应急响应培训和模拟演练，确保应急预案的有效性；
b) 应能够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) 应建立协同机制，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) 应制定访问控制策略，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) 应实施持续的安全验证措施，对用户和设备的身份进行鉴别，确保只有经过授权的实体才能访问算力网资源；

c) 应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 持续运行

a) 应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，以保障关键业务的持续运行；

b) 应确保在安全事件发生时，能够快速切换到维持算力网关键业务最小化运行的模式；

c) 应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。

6.2.3 控损恢复

6.2.3.1 损失控制

a) 应将算力网划分为相互隔离的区域，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，需要保障的关键业务功能；

b) 应遵循最小化授权原则，控制不同人员的操作维护权限；

c) 应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。

6.2.3.2 冗余配置

a) 算力网中关键业务的网络应实施冗余机制，包括硬件冗余、软件冗余、安全冗余等；

b) 应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) 应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。

d) 应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。

6.2.3.3 业务恢复

a) 应具备在算力网遭遇安全事件或故障后快速恢复能力，包括数据恢复、系统重建和服务恢复等；

b) 应准备必要的资源，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；

c) 基于算力网中系统或业务数据的重要性，应提供异地备份功能，利用网络将重要业务数据实时备份至备份场地；

d) 应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 重构适应

6.2.4.1 业务重构

a) 应保障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) 应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；

c) 应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。

6.2.4.2 动态适应

a) 应自动识别受损组件或节点，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，应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；
c) 根据运行环境变化和威胁态势，动态调整网络结构、访问控制策略及安全防护机制，支持基于威胁情报的网络路由动态切换和安全策略自动更新；
d) 监测到重大安全事件或业务需求变更时，可触发网络结构动态调整，调整范围包括路由策略、防火墙规则、区域划分等。

6.2.4.3 安全免疫

a) 应根据运行环境变化和威胁环境变化，利用人工智能、大数据等技术手段，通过自动化的方式构建自身安全能力，智能构建安全防御体系，有效抵御网络攻击；
b) 宜具备算力网中各类资产对于安全威胁的自身免疫能力，对程序进行保护，阻断非法进程运行。

7 算力网资源安全要求

7.1 算力节点安全

a) 应明确算力节点接入算力网的安全标准，对其安全性进行评估，并依据符合的安全标准标注算力资源；
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) 应支持节点隔离，如发现节点存在风险及时采取隔离措施，隔离后需进行安全评估，确认风险消除后可重新接入；
e) 对节点内运行的操作系统及应用软件，应建立白名单机制并定期扫描恶意代码；
f) 宜实施固件完整性校验和版本管控，防范固件篡改风险。

7.2 算力网通信安全

a) 应明确算力节点接入算力网的通信标准，并对其进行安全评估；
b) 应支持资源编排，算力网络通信流量按照规划的路径传输；
c) 应对算力网不同算力节点之间通信进行流量检测、异常行为检测，及时发现并防范报文篡改、漏洞攻击等攻击行为。

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保护，防止关键信息在发送过程中出现泄露；

c) 应实施算力资源隔离措施，将不同用户、不同安全等级的算力资源进行隔离，确保资源访问边界清晰；

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) 应实时监控算力资源的使用情况和性能状态，包括算力节点的任务分配情况、资源占用情况等；

f) 应建立审计机制，记录用户对算力资源的访问和关键操作。

8.2 资源编排安全

a) 应充分考虑安全等级等安全性因素，制定算力资源编排策略，并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；

c) 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，对其安全能力进行动态评估、划分安全等级；

b) 应支持对计算任务的安全性评估，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；

c) 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，应保护用户敏感数据以防泄露。

8.4 计量计费安全

a) 应使用密码技术保护度量数据与标识信息，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。

9 算力网监测平台安全要求

9.1 检测管理

a) 应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) 算力节点接入前应进行安全准入检测，并在算力节点加入算力网络后对其进行定期安全检测；

c) 应提供对算力节点镜像的安全管理能力，包括镜像可信检测、镜像扫描和基线核查、镜像完整性校验、镜像权限和访问控制。

9.2 运维管理

a) 应支持算力节点信息的访问和操作启动授权保护，重要操作需双因子认证，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；

b) 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；

c) 应保存算力网相关系统的登录、登出、维护操作等日志信息，并定期开展算力网运维相关日志的安全审计。

9.3 安全监测

a) 应对算力网中的资源访问和操作进行实时监测，记录和分析日志信息，及时发现和处理安全事件；

b) 应采用入侵检测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) 应通过限制算力用量、终止算力使用、拒绝算力请求或降低算力用户信用等措施对非法算力使用行为进行管控；

b) 应对算力网中的安全事件进行处置，明确事件原因、影响范围、应对措施、处置结果，并对算力网中安全处置结果进行复核，涉及重大安全事件的应按规定向相关部门报告。

10 算力网运营安全要求

10.1 运营门户安全

a) 门户展示敏感信息时应脱敏，防止敏感信息泄露；

b) 门户网站的访问应采用加密传输，防止数据泄密和中间人攻击；

c) 应实施身份认证和访问控制机制，防止未授权访问；

d) 应定期进行安全扫描、漏洞评估和渗透测试，确保门户的安全性；

e) 应对门户的关键页面实施防篡改机制，并记录操作日志；

f) 应定期审计门户访问日志，检测高频访问、暴力破解等异常行为。

10.2 算力交易安全

a) 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，做到交易过程可审计；

b) 应支持算力交易过程的多方签名验证，确保交易合法性；

c) 算力交易账单与结算等日志应加密存储，仅限授权人员访问，并满足可追溯要求；

d) 应建立算力交易风险分级防控机制，对于低风险交易采用自动化风控模式，对于中高风险需人工复核，处置记录存档备查。

10.3 产品管理安全

a) 算力网产品发布前应通过安全测试，如渗透测试、API 接口鉴权验证、代码审计等；

b) 下架产品应清理关联数据，避免残留敏感信息。

10.4 算力并网安全

a) 应对并入的算力节点实施严格的资源注册认证，确保算力来源可信；

b) 应对接入算力进行安全评级，不满足安全要求的资源禁止并网。

10.5 用户管理安全

a) 应对算力网访问主体进行身份标识，实现算力网用户、算力网资源等实体的全面身份化；
b) 应遵循最小化原则，采用基于角色的访问控制，角色权限要按需动态调整；
c) 应强制用户账号密码复杂度策略，定期提示更换密码；
d) 运维人员权限应按需分配，禁用默认超级管理员账号，离职人员账号应及时回收，会话设置有效期；
e) 应记录用户关键操作，留存日志不少于 6 个月。

10.6 运营管理安全

a) 电子合同应进行数字签名，并加密存储；
b) 订单数据脱敏后应开放查询，敏感操作应审批留痕；
c) 运营数据应每日增量备份，核心数据异地容灾。

11 算力网数据安全要求

11.1 数据采集

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) 应对数据采集过程采取必要的安全管控措施，如数据脱敏、数据水印等措施；
d) 数据采集应获得数据提供方的明确授权，符合最小必要原则，对涉及个人信息的数据，应明确告知采集目的、范围及用途并获得同意。

11.2 数据传输

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) 应对数据传输过程中的状态、频率等进行监控，并在出现异常时进行提示。

11.3 数据处理与使用

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) 应对用于调试、测试的重要数据进行数据脱敏；
c) 应监测数据处理和使用过程中的异常行为，并在出现异常时即时告警；
d) 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、操作时间等关键要素。

11.4 数据存储

a) 应制定数据存储策略，并对数据存储合规性进行评估；
b) 应对重要数据进行加密存储；
c) 应对数据存储建立冗余及备份机制；
d) 应数据存储的异常状态监测，并在出现异常时进行即时告警。

11.5 数据销毁

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

a） 应制定审计策略，明确审计频率，合规性评估需验证审计覆盖完整性；
b） 应对数据使用全程访问过程进行审计；
c） 应对审计、运维角色的增、删、改、查等进行操作行为审计；
d） 应对数据审计记录进行登记并归档。

11.7 数据安全应急

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、算力资源、应用、数据等实时监测，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） 应定期组织网络安全应急演练，并对演练记录进行保存。

11.8 数据安全评估

a） 应制定数据安全评估策略，并对其合规性进行评估；
b） 应支持主动探测与被动发现等方式识别在网数据资产、检测数据风险；
c） 应具备对数据风险评估、检测的技术手段，包括但不限于数据识别、漏洞扫描、合规检查、安全策略有效性验证等；
d） 应定期组织数据安全风险评估，评估内容应包括数据安全管理制度、数据安全管理流程、数据安全保护措施等；
e） 对于加工和处理核心重要数据的算力网资源，应每年至少开展一次数据安全评估，发生重大数据安全事件或系统重大变更后应重新评估。