TC609

全国数据标准化技术委员会技术文件

TC609-6-2025-XX

数据基础设施 安全能力通用要求

Data infrastructure—General requirements for security capability

（征求意见稿）

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：

数据基础设施 安全能力通用要求

1 范围

本文件规定了数据基础设施安全能力的通用要求，以功能视角下的数据基础设施架构为基础，结合安全保障层的内容对流通利用设施层、算力设施层、网络设施层的各组件提出了安全能力要求。

本文件适用于数据基础设施的规划、建设、运营和评估等各个环节，旨在为数据基础设施相关方提供全面的安全指导，确保数据的安全性、保密性、完整性和可用性。

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。

NDI—TR—2025—01 数据基础设施参考架构

NDI—TR—2025—02 数据基础设施互联互通基本要求

NDI—TR—2025—03 数据基础设施用户身份管理和接入规范

NDI—TR—2025—04 数据基础设施标识要求

NDI—TR—2025—05 数据基础设施连接器技术要求

NDI—TR—2025—06 数据基础设施数据目录描述规范

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据基础设施 datainfrastructure

从数据要素价值释放的角度出发，面向社会提供数据采集、汇聚、传输、加工、流通、利用、运营、安全服务的一类新型基础设施，是集成硬件、软件、模型算法、标准规范、机制设计等在内的有机整体。

3.2

安全能力 securitycapability

数据基础设施在抵御安全威胁、防范安全风险、保障数据安全等方面的防护能力与应对能力。

3.3

数据流通利用 datacirculationandutilization

数据在不同主体之间进行合法、合规、有序地流动与使用，以充分发挥数据的价值。

3.4

数据资源 dataresources

具有价值创造潜力的数据的总称，通常指以电子化形式记录和保存、可机器读取、可供社会化再利用的数据集合。

3.5

数据安全 datasecurity

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.6

数据处理 dataprocessing

包括数据的收集、存储、使用、加工、传输、提供、公开等。

3.7

数据流通 datacirculation

数据在不同主体之间流动的过程，包括数据开放、共享、交易、交换等。

3.8

数据交易 datatrading

数据供方和需方之间进行的，以特定形态数据为标的，以货币或者其他等价物作为对价的交易行为。

3.9

数据治理 datagovernance

提升数据的质量、安全、合规性，推动数据有效利用的过程，包含组织数据治理、行业数据治理、社会数据治理等。

3.10

数据分析 dataanalysis

通过特定的技术和方法，对数据进行整理、研究、推理和概括总结，从数据中提取有用信息、发现规律、形成结论的过程。

3.11

隐私保护计算 privacypreservingcomputation

在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一类信息技术，保障数据在产生、存储、计算、应用、销毁等数据流转全过程的各个环节中“可用不可见”。隐私保护计算的常用技术方案有安全多方计算、联邦学习、可信执行环境、密态计算等。常用的底层技术有混淆电路、不经意传输、秘密分享、同态加密等。

3.12

安全多方计算 securemulti-partycomputation

在一个分布式网络中，多个参与实体各自持有秘密数据，各方希望以这些数据为输入共同完成对某函数的计算，而要求每个参与实体除计算结果、预期可公开的信息外均不能得到其他参与实体的任何输入信息。主要研究针对无可信第三方情况下，安全地进行多方协同的计算问题。

3.13

可信执行环境 trustedexecutionenvironment

基于硬件级隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。

3.14

密态计算 cryptographiccomputing

通过综合利用密码学、可信硬件和系统安全相关技术，实现计算过程数据可用不可见，计算结果能够保持密态化，以支持构建复杂组合计算，实现计算全链路保障，防止数据泄漏和滥用。

3.15

区块链 blockchain

是分布式网络、加密技术、智能合约等多种技术集成的新型数据库软件，具有多中心化、共识可信、不可篡改、可追溯等特性，主要用于解决数据流通过程中的信任和安全问题。

4 数据基础设施安全能力框架

4.1 概述

数据基础设施安全能力通过安全能力维度、数据活动维度和数据基础设施维度三个层面构成了一个“覆盖全面、要求清晰”的立体结构，如图1所示。

a) 安全能力维度：明确数据基础设施在组织建设、制度流程、技术工具、人员能力上的安全属性；
b) 数据活动：从数据生命周期角度，识别数据基础设施不同组件所涉及的数据处理活动，为提出针对性安全要求提供基础；
c) 数据基础设施维度：数据基础设施维度关注承载设施自身的安全，包括身份、目录和标识、全域功能节点、区域/行业功能节点、接入连接器、算力和网络等；

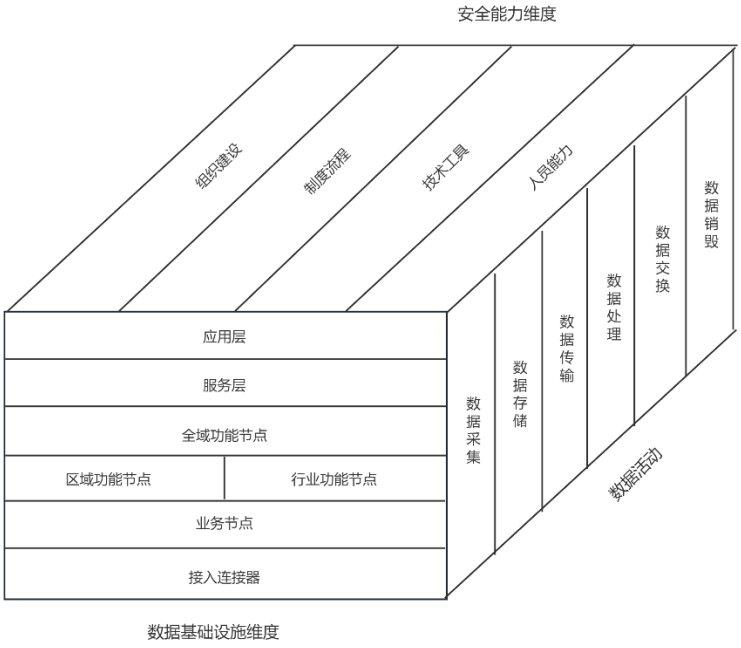

图 1 数据基础设施安全能力要求架构图

4.2 安全总体原则

4.2.1 整体性与动态性原则

数据基础设施涉及多方主体，应采取整体视角进行防护。安全策略和技术措施应具备动态适应能力，能够应对不断变化的业务场景、技术架构和安全威胁，实现从静态防御向动态保护的转变。

4.2.2 全生命周期覆盖原则

安全能力应贯穿数据从采集到最终销毁的全生命周期。应在每个环节内置相应的安全控制措施，形成无缝衔接、无死角的闭环防护链条，确保数据在任何状态下都能得到有效保护。

4.2.3 内生安全原则

将安全能力作为数据基础设施的核心组成部分进行同步规划、同步建设和同步运行，而非作为外部附加功能。安全应深度融入技术架构、业务流程与系统组件中，提供原生的、内建的防护能力。

4.2.4 体系化与协同防护原则

构建一个标准化、多层次、全方位的安全防护体系，系统性地保障数据基础设施相关的网络、算力、数据、应用等各个层面的安全。各安全组件与能力应协同联动，形成纵深防御，共同抵御来自内部和外部的各类风险与威胁。

5 组织建设能力要求

5.1.1 岗位设置

数据基础设施的岗位设置应满足以下要求：

a) 应成立指导和管理网络安全工作的委员会或领导小组,其最高领导由单位主管领导担任或授权，总体负责数据安全工作的统筹组织、指导推进和协调落实，明确数据安全管理部门，协调机构内部数据安全管理资源调配；

b) 委员会成员应至少包含主要部门的主要负责人，负责数据安全相关工作的实施、相关政策和制度的制定评审工作，保障数据安全管理工作所需资源，并设立数据安全管理专职岗位，负责日常数据安全管理工作，具体如下：
   1) 主要部门应至少包括数据安全管理、信息科技、业务、法务、合规、风险管理、稽核审计、人事部门等相关部门；
   2) 制定、发布和更新本机构数据安全管理制度、规程与细则；
   3) 组织开展本机构数据分级工作，识别并维护数据资产清单；
   4) 制定、签发、实施、定期更新隐私政策和相关规程；
   5) 监督本机构内部，以及本机构与外部合作方数据安全管理情况；
   6) 在数据基础设施发布前组织开展数据安全评估,避免不当的数据采集、使用、共享等行为,如与产品或服务功能及隐私政策不符等情况。

c) 应设立网络安全管理工作的职能部门,设立安全主管、安全管理各个方面的负责人岗位,并定义各负责人的职责，该岗位应履行以下工作职责：
   1) 根据数据安全相关策略和规程，落实本部门数据安全防护措施；
   2) 经授权审批程序后，为获得授权的各相关方分配数据权限；
   3) 对本部门数据脱敏、对外提供等关键活动的数据安全控制有效性进行确认；
   4) 配合执行数据相关安全评估及技术检测等工作；
   5) 制定本部门数据安全应急预案，并定期开展数据安全应急演练，依据演练结果，修订数据安全应急预案；
   6) 处置本部门有关数据安全事件；
   7) 依据数据安全管理有关制度规范，记录本部门数据活动日志。

d) 应设立系统管理员、审计管理员和安全管理员等岗位,并定义部门及各个工作岗位的职责，该岗位应履行以下工作职责：
   1) 根据本机构数据相关业务实际情况，确定相应审计策略及规范，包括但不限于审计周期、审计方式、审计形式等内容；
   2) 监督数据安全政策、方针的执行；
   3) 公布投诉、举报方式等信息，并及时受理数据安全和隐私保护相关投诉和举报；
   4) 开展数据安全内部审计和分析，发现并反馈问题和风险，并对机构后续相关整改工作进行监督；
   5) 配合开展外部审计相关的组织和协调工作。

5.1.2 人员配备

数据基础设施的人员配备应满足以下要求：

a) 应配备一定数量的系统管理员、审计管理员和安全管理员等；
b) 应配备专职安全管理员，不可兼任。

6 制度流程能力要求

6.1 制度管理要求

数据基础设施参与方具有安全管理制度的能力，应满足以下要求：

a) 数据基础设施参与方应依据《网络安全法》《数据安全法》和《个人信息保护法》及关键信息基础设施安全保护条例、国家商用密码管理、网络安全等级保护、关键信息基础设施安全保护等，制定明确且全面的安全方针。安全方针不仅覆盖数据全生命周期的各个环节，而且应与基础设施的整体业务目标和发展方向保持一致，建立管理规范，将其传达至所有相关方并监督执行；
b) 数据基础设施运营者应建立覆盖以下层级的制度：
    1) 战略级：数据安全方针、数据安全战略规划；
    2) 管理级：数据访问控制、应急响应等管理制度；
    3) 操作级：数据采集、存储、传输、处理、销毁等环节的操作规程。

6.2 流程管理要求

6.2.1 流程设计原则

流程设计的原则应满足以下要求：

a) 应基于最小权限原则设计安全流程；
b) 关键流程应设计审批环节和记录要求；
c) 流程设计需覆盖数据全生命周期，并与业务场景深度融合。

6.2.2 数据业务流程设计

组织应基于数据生命周期建立规范的数据业务管理制度，应满足以下要求：

a) 建立数据分类分级制度，明确标识规则及对应安全措施；
b) 制定数据采集审批流程，确保合法性、最小必要性和知情同意；
c) 数据源鉴别与记录机制。
d) 明确传输加密算法、密钥管理及通道安全要求；
e) 制定网络冗余和故障恢复流程。
f) 规范存储媒体的访问、使用及销毁流程；
g) 制定数据库权限管理、加密存储及备份恢复制度。
h) 明确敏感数据脱敏场景、方法及使用限制；
i) 数据处理环境安全规范。
j) 制定数据共享评估机制，明确责任方及保密协议；
k) 规范接口调用身份鉴别、访问控制及审计要求。
l) 建立数据及存储媒体的安全销毁审批与监督机制。

6.3 持续改进机制

6.3.1 评审与更新

组织应建立规范的评审与更新制度，应满足以下要求：

a) 每年至少开展一次制度流程的全面评审；

b) 保留制度修订记录。

6.3.2 监督与考核

组织应建立规范的监督与考核制度，应满足以下要求：

通过内部审计验证流程有效性。

7 技术工具能力要求

7.1 目录安全

数据基础设施的数据目录安全应满足以下要求：

a) 数据目录的内容，以及编制、管理和应用的过程需严格遵守国家法律法规和相关政策要求，如《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等；

b) 应构建数据目录责任制度，详细规定各环节的操作规范与安全准则，明确数据安全责任主体，并清晰责任分工，建立追责问责机制；

c) 应对数据目录中提交样例数据部分涉及个人隐私的数据进行脱敏处理，确保数据目录中不泄露个人隐私；

d) 应根据不同安全等级的数据，数据资源管理责任主体对数据目录及其对应数据样例设置不同的公开范围，拟公开的信息，应未涉及任何国家安全与秘密的信息；

e) 应定期进行数据目录安全评估和风险监测，确保数据目录的安全性。

f) 在建立覆盖全国的分布式数据目录时，应保障目录数据的完整性、一致性、保密性和可用性，防止未经授权的访问、查询和修改，

g) 数据基础设施体系中，数据目录传输所采用的设备应符合有关设备的安全要求；

h) 应对已限制访问的数据目录，设置访问控制体系，防止未经授权的访问和信息泄露。

7.2 身份安全

7.2.1 基本要求

a) 运行维护组织与责任制度：全域功能节点、区域/行业功能节点、业务节点及接入连接器应设立专责的运行维护组织，明确各类运维岗位职责，建立日常值守、问题响应、系统变更等管理流程，保障身份管理系统持续、稳定运行。

a) 应急预案与演练机制：应制定包含故障恢复、数据泄露、非法接入、系统攻击等场景的应急预案，并定期组织演练和效果评估，提升故障处置能力和业务恢复效率。

b) 日志记录与保留：应确保网络设备、主机设备、应用系统及数据库系统具备日志采集功能。日志记录内容包括但不限于用户登录、身份变更、凭证签发、访问行为等，保存时间不少于 180 天，并应支持归档和审计溯源。

c) 数据一致性与冗余清理：应定期清理和校验用户数据、系统数据，排查冗余记录与失效身份，确保数据结构完整、状态准确、权限匹配。

d) 跨域互信保障机制：各级节点应建立身份状态同步机制，确保注销、变更、吊销等关键状态可在全网范围内实时感知与一致性更新，避免因信息不同步导致的信任失效或安全漏洞。同时，应坚持跨域节点的“三统一”原则，即统一标准、统一流程、统一接口，推进用户信息的集中管理和全网互认；在跨域信息同步过程中，应采用分级同步策略，仅同步必要的基础信息，敏感信息由注册节点进行安全隔离和保管，确保用户隐私安全。

e) 用户隐私保护与数据采集合规：应严格遵循国家有关个人信息保护法律法规和数据安全要求，制定并执行数据最小化原则，限制对用户敏感信息的采集范围和使用场景，确保仅收集为身份管理所必需的信息。应完善用户授权和知情机制，保障用户对其身份信息采集、使用、存储和删除等行为的知情权、同意权和查询权，确保用户隐私安全与数据使用合法合规。

7.2.2 账户安全措施

a) 登录失败限制：限制登录失败次数，当登录失败次数达到一定限制时，自动锁定账户并触发安全通知，管理员可解锁或用户自助验证身份后恢复。

b) 多因素认证机制：对高权限用户或关键操作应启用多因素认证机制，结合动态口令、指纹、人脸识别等多因子手段增强安全性。

7.2.3 数据安全措施

a) 数据定期备份与离线存储：定期对系统和数据进行备份，并生成加密存储，以防止数据丢失或损坏。备份数据定期验证可用性。

b) 数据加密：使用符合国家和密码行业标准的密码算法或基于硬件级安全保护模块对平台数据进行加密，防止数据在存储、传输过程中被窃取和篡改。

c) 访问控制最小权限原则：对数据访问实施严格控制，结合最小权限原则和角色访问控制等机制，分级分域管理数据，，防止未经授权的用户访问或泄露数据。

d) 硬件级安全保护：应支持使用硬件级安全模块对密钥和敏感数据进行硬件隔离和安全存储，防止物理攻击和非法访问。同时，支持数据存储、密钥管理、数字签名及数据加密等功能，保障数据的机密性、完整性和可用性。

e) 敏感信息分离存储：对用户名、口令等敏感信息可采用安全硬件模块或安全容器进行分离存储，进一步降低数据安全风险。

7.2.4 应用软件安全措施

a) 全生命周期安全管理：从开发、测试、部署到运维，均应嵌入安全审查流程，包括代码审计、渗透测试、第三方组件漏洞评估等环节。

b) 应用软件进行更新和维护：定期更新和维护应用软件，包括操作系统和应用程序，以修复已知的漏洞和安全问题。

c) 安全开发和测试：在应用软件的开发和测试过程中，考虑安全因素，遵循安全最佳实践和安全编码标准。

d) 补丁管理与版本控制：应建立安全补丁发布机制，对操作系统、中间件、应用软件进行版本迭代记录和补丁推送。重大漏洞应在 24 小时内完成应急修复或风险隔离。

7.2.5 数据需求分级与认证等级要求

a) 业务节点、区域/行业功能节点应结合数据基础设施中的数据类型、业务敏感性及访问风险，对数据访问需求进行分级管理，并基于分级结果明确相应的用户身份认证等级要求。

b) 数据需求分级可参考以下划分示例（可根据行业特性和安全需求进一步细化）：

- 低风险数据（如基础信息、非敏感统计数据）：对应0级认证（无实名认证或最低实名核验要求）。

- 中等风险数据（如敏感用户信息、部分业务操作数据）：对应1级认证（身份证或社保卡实名认证）。

- 高风险数据（如核心业务数据、重要资源操作权限）：对应2级及以上认证（基于身份证实名认证+人脸识别或其他多因子认证）。

c) 认证等级应与业务需求和数据风险相适配，高敏感度数据访问必须具备相应的认证等级要求，不得以低认证等级替代高认证等级访问，确保数据安全性和合规性。
d) 认证等级划分标准应由区域/行业功能节点根据实际应用场景及行业监管要求制定，并报全域功能节点备案，确保认证策略的统一性和可扩展性。
e) 当认证等级发生调整时，系统应具备相应的动态适配机制，及时同步认证状态变更，保障用户体验与安全合规并重。

7.2.6 记录与审计措施

a) 身份全生命周期记录：全域功能节点、业务节点、区域/行业功能节点和接入连接器应对用户身份生成、更新、使用、授权、销毁等全生命周期行为建立详尽日志，记录内容应包括时间、操作人、操作对象、结果与 IP 信息等。
b) 日志不可篡改存储：应采用链式哈希、区块链或只读归档机制保障审计日志的不可篡改性，支持事后取证与合规监管。
c) 定期审计与行为分析：明确安全审计策略，定期对日志记录进行审计，对身份异常使用、越权访问、操作频率异常等行为进行识别与报警。
d) 审计记录安全备份与多地分发：审计日志应定期加密备份至异地安全节点，避免受到未预期的删除、修改和覆盖。

7.2.7 管理安全要求

i) 数据目录的内容，以及编制、管理和应用的过程需严格遵守国家法律法规和相关政策要求，如《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等；
j) 应构建数据目录责任制度，详细规定各环节的操作规范与安全准则，明确数据安全责任主体，并清晰责任分工，建立追责问责机制；
k) 应对数据目录中提交样例数据部分涉及个人隐私的数据进行脱敏处理，确保数据目录中不泄露个人隐私；
l) 应根据不同安全等级的数据，数据资源管理责任主体对数据目录及其对应数据样例设置不同的公开范围，拟公开的信息，应未涉及任何国家安全与秘密的信息；
m) 应定期进行数据目录安全评估和风险监测，确保数据目录的安全性。

7.3 标识安全

标识码是身份确认、节点平台互联的关键，应满足标识安全性要求：

a) 标识使用环境安全：涉及到标识的传输、存储时应符合国家信息安全等级保护、商用密码应用安全性评估等要求。

b) 标识管理设施安全：涉及标识赋码、查询或解析的平台节点，宜建立标识码冗余检测与纠错机制、唯一性校验、高并发处理、全链路日志审计及容灾恢复等处理方案。

7.4 功能节点

数据基础设施业务节点，安全性应满足以下要求：

a) 等保安全：应至少满足GB/T22239—2019中规定的第三级安全要求；
b) 完整性要求：应采用密码技术、区块链、可信技术保证身份管理信息、接入连接器管理信息、业务平台管理信息、数据资源和产品登记信息、目录管理信息和标识管理信息的完整性，防止未授权篡改；
c) 机密性要求：应具有安全的存储环境确保身份管理信息、接入连接器管理信息、业务平台管理信息、数据资源和产品登记信息、目录管理信息和标识管理信息中敏感信息的机密性，防止未授权泄露；
d) 访问控制：应建立访问权限申请和审核批准机制，并具有访问控制组件或访问控制代理技术对访问的终端设备、系统进行控制，以及实际操作和申请操作进行验证，保证实际操作与申请并审批的操作是一致的；
e) 身份鉴别：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对管理人员、运维人员、用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；
f) 审计：应对数据的访问权限和实际访问控制情况进行定期审计，至少每半年1次对访问权限规则和已授权清单进行复核，及时清理已失效的账号和授权；
g) 接口安全：应构建标准化、规范化的交互接口，并对接口进行严格的安全设计与管理，具备身份认证、权限控制、防重放攻击、防数据泄露等安全能力，确保数据基础设施互联互通的安全性。
h) 应保证功能节点的业务处理能力满足身份管理、接入连接器管理、数据资源和产品登记管理的业务高峰期需求，如身份查询、目录同步、连接器注册等管理业务。

7.5 接入连接器

7.5.1 标识和鉴别安全

接入连接器的标识和鉴别能力安全性应满足以下要求：

a) 接入连接器应基于数字证书实现双向身份验证、唯一标识比对等方式核验所对接的接入连接器身份，确保对接的接入连接器身份可信；
b) 接入连接器可支持对用户的多因素认证（如动态口令、短信验证码等）和密钥核验等方式，验证用户身份的真实性，确保只有授权用户能够访问连接器设备；
c) 应保障用户和接入连接器自身的标识和鉴别信息在传输和存储过程中的保密性和完整性；
d) 使用口令鉴别方式时，应提供口令的强度验证和定期更换功能，并支持首次接入连接器时强制修改默认口令。

7.5.2 访问控制安全

接入连接器的访问控制能力安全性应满足以下要求：

a) 对接入连接器的用户分配账户和权限，区分管理员角色，实现管理权限相互制约；
b) 对接入连接器自身应支持通过配置访问控制策略、白名单管控等方式，控制网络访问权限；
c) 应配备必要的网络安全能力，防止被攻击或入侵。

7.5.3 系统安全

接入连接器系统安全性应满足以下要求：

a) 支撑接入连接器的软件代码应经过严格的安全扫描，不应包含已公开的中、高风险漏洞；
b) 应定期检查和更新依赖的第三方库、框架等组件，防止因组件漏洞导致的安全风险；
c) 接入连接器的运行环境应具备安全防护机制，防止恶意软件入侵或未经授权的访问。在启动与升级部署过程中，应具备版本完整性校验功能，防止软件被篡改；
d) 接入连接器应对安全事件数据进行完整记录，并上传至区域功能节点；
e) 接入连接器的安全性能宜通过第三方专业机构安全评估。

7.5.4 数据安全

接入连接器的数据安全能力应满足以下要求：

a) 采集安全：应具有摘要、消息认证码、数字签名等密码技术确保从本地接入的数据资源的完整性和机密性；应对数据采集过程进行日志记录，并采取技术措施确保信息来源的可追溯性；
b) 数据传输：应具有校验技术或密码技术保证数据在连接器和连接器之间，连接器和功能节点之间，连接器和业务节点之间的数据在输过程中的完整性。应具有密码技术保证数据在连接器和连接器之间，连接器和功能节点之间，连接器和业务节点之间的数据在输过程中的机密性；
c) 数据存储安全：应采取加密等技术措施保证数据存储的保密性；
d) 数据访问安全：问应建立访问权限申请和审核批准机制，并具有访问控制组件，保证实际操作与申请并审批的操作是一致的；
e) 数据加工安全：应具有隐私保护计算、沙箱技术等保障数据加工过程的安全性，确保数据不会被篡改、泄露、滥用等；
f) 数据使用安全：应具有隐私保护计算、使用控制技术、数字合约技术等保障数据使用的安全，确保数据不会被滥用；
g) 数据删除安全：应具有数据产品的删除的能力，使其保持不可被检索、访问的状态。

7.5.5 用户信息安全

接入连接器的用户信息安全能力应满足以下要求：

a) 用户信息应加密保存在接入连接器内，不应导出；
b) 连接器的运维和管理人员不能在非授权的情况下获取用户信息。

7.6 业务节点

数据基础设施业务节点，如可信数据空间，安全性应满足以下要求：

a) 相关信息系统应至少满足GB/T22239—2019中规定的第三级安全要求；
b) 完整性要求：应采用密码技术、区块链、可信技术保证身份管理信息、接入连接器管理信息、业务平台管理信息、数据资源和产品登记信息、目录管理信息和标识管理信息的完整性，防止未授权篡改；
c) 机密性要求：应具有安全的存储环境确保身份管理信息、接入连接器管理信息、业务平台管理信息、数据资源和产品登记信息、目录管理信息和标识管理信息中敏感信息的机密性，防止未授权泄露；
d) 访问控制：应建立访问权限申请和审核批准机制，并具有访问控制组件或访问控制代理技术对访问的终端设备、系统进行控制，以及实际操作和申请操作进行验证，保证实际操作与申请并审批的操作是一致的；
e) 身份鉴别：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对管理人员、运维人员、用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；

f） 审计：应对数据的访问权限和实际访问控制情况进行定期审计，至少每半年1次对访问权限规则和已授权清单进行复核，及时清理已失效的账号和授权；
g） 接口安全：应构建标准化、规范化的交互接口，并对接口进行严格的安全设计与管理，具备身份认证、权限控制、防重放攻击、防数据泄露等安全能力，确保数据基础设施互联互通的安全性。
h） 应保证功能节点的业务处理能力满足身份管理、接入连接器管理、数据资源和产品登记管理的业务高峰期需求，如身份查询、目录同步、连接器注册等管理业务。

7.7 网络和算力

7.7.1 网络

数据基础设施网络应满足以下要求：
a） 应保证网络设备的业务处理能力满足业务高峰期需要；
b） 应保证网络各个部分的带宽满足业务高峰期需要；
c） 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
d） 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术
e） 隔离手段；
f） 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

7.7.2 算力安全

数据基础设施算力安全性应满足以下要求：
g） 提供计算资源的安全隔离机制，支持通用算力、智能算力、超级算力等多元异构算力的安全协同。
h） 在实现跨平台、跨层级、跨区域的算力资源统一调度时，应确保调度指令和过程的安全，防止算力资源被劫持或滥用，以保障算力资源的科学布局与东西部算力的安全协同；
i） 对计算任务采取严格身份认证、访问控制和数据加密，确保计算任务的安全性和隐私性。

8 人员能力要求

8.1 人员录用

数据基础设施的人员录用应满足以下要求：
a） 应指定或授权专门的部门或人员负责人员录用；
b） 应对被录用人员的身份、安全背景、专业资格或资质等进行审查,对其所具有的技术技能进行考核，同时在录用员工前，需要进行必要的背景调查；
c） 应与被录用人员签署保密协议,与关键岗位人员签署岗位责任协议，应满足以下要求：
4） 对数据安全关键岗位制定统一的保密协议，并与可接触保护等级较高数据的员工以及从事数据安全关键岗位的员工签署保密协议；
5） 识别机构数据安全关键岗位，并与其签署数据安全岗位责任协议，数据安全关键岗位包括但不限于：
——数据安全管理岗位、审计岗位；
——业务操作与信息技术操作特权账户所有者；
——数据各级权限审批岗位；
——重要数据处理岗位；

——信息系统开发、测试岗位人员；
——因业务需要，需高频和(或)大批量接触3级及以上数据的岗位人员；
——外部数据采购岗位；
——其他金融业机构识别的数据安全关键岗位。

6) 在发生人员调离岗位时，立即完成相关人员数据访问、使用等权限的配置调整，并明确有关人员后续的数据保护管理权限和保密责任；若有关人员调整后的岗位不涉及数据的访问与处理的，明确其继续履行有关信息的保密义务要求。

7) 与员工终止劳动合同时，立即终止并收回其对数据的访问权限，明确并告知其继续履行有关信息的保密义务要求，并签订保密承诺书。

8) 建立外部人员管理制度，对允许被外部人员访问的系统和网络资源建立数据存取控制机制、认证机制，列明所有外部用户名单及其权限，加强对外部人员的数据安全要求和培训，必要时签署保密协议。

8.2 人员离岗

数据基础设施的人员离岗应满足以下要求：

a) 应及时终止离岗人员的所有访问权限,取回各种身份证件,钥匙、徽章等以及机构提供的软硬件设备；

b) 应办理严格的调离手续,并承诺调离后的保密义务后方可离开。

8.3 安全意识教育和培训

数据基础设施的安全意识教育和培训应满足以下要求：

a) 应对各类人员进行安全意识教育和岗位技能培训,并告知相关的安全责任和惩戒措施；

b) 应针对不同岗位制定不同的培训计划,对安全基础知识、岗位操作规程等进行培训，并至少满足以下要求：

1) 按照培训计划定期开展数据安全意识教育与培训，培训内容包括但不限于国家有关法律法规、行业规章制度、技术标准，以及金融业机构内部数据安全有关制度与管理规程等内容，并对培训结果进行评价、记录和归档；

2) 对密切接触高安全等级数据的人员定期开展数据安全意识教育和培训，培养办公数据定期删除意识，并定期开展数据删除自查工作；

3) 每年至少对数据安全管理专职与关键岗位人员进行1次数据安全专项培训；

4) 至少每年1次或在隐私政策发生重大变化时，对数据安全关键岗位上的人员开展专业化培训和考核，确保人员熟练掌握隐私政策和相关规程。

c) 应定期对不同岗位的人员进行技能考核；

d) 在数据相关人员管理及关键岗位设置方面，应进一步加强管理，并应对接触高安全等级数据的人员及其岗位进行审批和登记，并定期对这些人员行为进行安全审查；

e) 数据库管理员、操作员及安全审计人员等岗位应设立专人专岗，并实行职责分离；必要时特权账户所有者、关键数据处理岗位等数据安全关键岗位应设立双人双岗，强化数据安全管理。

8.4 外部人员访问管理

数据基础设施的外部人员访问管理应满足以下要求：

a) 应在外部人员物理访问受控区域前先提出书面申请,批准后由专人全程陪同,并登记备案；

b) 应在外部人员接人受控网络访问系统前先提出书面申请,批准后由专人开设账户、分配权限，并登记备案；

c) 外部人员离场后应及时清除其所有的访问权限；
d) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

参 考 文 献

[1] GB/T31168-2014《信息安全技术云计算服务安全能力要求》
[2] GB/T35274-2017《信息安全技术大数据服务安全能力要求》
[3] GB/T36323-2018《信息安全技术工业控制系统安全管理基本要求》
[4] GB/T35273-2017《信息安全技术个人信息安全规范》
[5] GB/T19715-2005《信息技术信息技术安全管理指南》
[6] GB/T37932-2019《信息安全技术 数据交易服务安全要求》
[7] GB/T37988-2019《信息安全技术数据安全能力成熟度模型》
[8] 《国家数据基础设施建设指引》
[9] 《关于建立公共数据资源授权运营价格形成机制的通知》
[10] 《公共数据资源登记管理暂行办法》
[11] 《公共数据资源授权运营实施规范（试行）》
[12] 《关于完善数据流通安全治理更好促进数据要素市场化价值化的实施方案》
[13] 《关于促进数据产业高质量发展的指导意见》
[14] 《关于促进企业数据资源开发利用的意见》
[15] 《可信数据空间发展行动计划（2024—2028年）》
[16] 《国家数据标准体系建设指南》
[17] 《“数据要素×”三年行动计划（2024—2026年）》
[18] 《关于深入实施“东数西算”工程加快构建全国一体化算力网的实施意见》
[19] 《中华人民共和国网络安全法》
[20] 《中华人民共和国个人信息保护法》
[21] 《关键信息基础设施商用密码使用管理规定》
[22] 《中华人民共和国数据安全法》
[23] 《银行保险机构数据安全管理办法》