数网信认证服务（北京）有限公司

大数据安全管理体系技术规范

文件编号：DNI-GZ-JS-64

技术规范编号：CTS DNIA999903-2026

文档版本：A/0

编制：技术部　　日期：2026.02.12

审核：杨舒　　日期：2026.02.12

批准：杨舒　　日期：2026.02.12

受控状态：受控文件

发布日期：2026 年 02 月 12 日

实施日期：2026 年 02 月 12 日

变更履历

日期	变更描述	版本/版次	审核	批准
2026.02.12	初始版发布	A/0	杨舒	杨舒

大数据安全管理体系技术规范

1.适用范围

本技术规范是我机构实施大数据安全管理体系认证的认证依据，也是申请大数据安全管理体系认证的组织建立、实施和持续改大数据安全管理体系的依据，同时，实施本技术规范也便于各组织有效、安全地应用大数据，采用有效技术和管理措施保障数据安全。

2.规范性引用文件

GB/T 7027—2002 信息分类和编码的基本原则与方法

GB/T 20984—2007 大数据安全技术 大数据安全风险评估规范

GB/T 25069—2010 大数据安全技术 术语

GB/T 31167—2014 大数据安全技术 云计算服务安全指南

GB/T 35274—2017 大数据安全技术 大数据服务安全能力要求

GB/T 22080-2025/ISO/IEC 27001:2022 网络安全技术 信息安全管理体系 要求

3.术语与定义

3.1

大数据 big data

具有数量巨大、种类多样、流动速度快、特征多变等特性，并且难以用传统数据体系结构和数据处理 技术进行有效组织、存储、计算、分析和管理的数据集。

3.2

组织 organization

由作用不同的个体为实施共同的业务目标而建立的结构。

注：组织可以是一个企业、事业单位、政府部门等。

3.3

大数据平台 big data platform

采用分布式存储和计算技术，提供大数据的访问和处理，支持大数据应用安全高效运行的软硬件 集合。

3.4

大数据环境 big data environment

开展大数据活动所涉及的数据、平台、规程及人员等的要素集合。

3.5

大数据活动 big data activity

组织针对大数据开展的一组特定任务的集合。

注：大数据活动主要包括采集、存储、处理、分发、删除等活动。

4 组织环境

4.1 理解组织及其环境

组织应确定与其意图相关的，且影响其达到大数据安全管理体系预期结果能力的外部和内部事项。

组织应确定气候变化[1]是否是一个相关事项。

注：对这些事项的确定，见 GB/T 24353—2022 中 5.4.1 建立外部和内部环境。

4.2 理解相关方的需求和期望

组织应确定：

a) 大数据安全管理体系的相关方；

b) 这些相关方的有关要求；

c) 哪些要求将通过大数据安全管理体系予以解决。

注 1:相关方的要求包括法律、法规和合同义务。

注 2.相关方可能提出与气候变化相关的要求

1) 有关气候变化的更多信息，见ISO和国际认可论坛(IAF)关于管理体系标准中增加气候变化因素的联合公报。

4.3 确定大数据安全管理体系范围

组织应确定大数据安全管理体系的边界及其适用性，以建立其范围。

组织应根据以下内容确定大数据安全管理体系范围：

a) 4.1 中提到的外部和内部事项；

b) 4.2 中提到的要求；

c) 组织实施的活动与其他组织实施的活动之间的接口和依赖关系。

范围应形成文件化信息并可用。

4.4 大数据安全管理体系

组织应按本文件的要求，建立、实现、维护和持续改进大数据安全管理体系，包括所需的过程及其相互 作用。

5 领导

5.1 领导和承诺

最高管理层应通过以下活动，证实其对大数据安全管理体系的领导和承诺：

a) 确保建立了大数据安全方针和大数据安全目标，并与组织战略方向一致；

b) 确保将大数据安全管理体系要求整合到组织的业务过程中；

c) 确保大数据安全管理体系所需资源可用；

d) 沟通有效大数据安全管理的重要性和符合大数据安全管理体系要求的重要性；

e) 确保大数据安全管理体系达到预期结果；

f) 指导并支持相关人员为大数据安全管理体系的有效性作出贡献；

g) 促进持续改进；

h) 支持其他相关管理角色在职责范围内证实其领导作用。

注：本文件中提到的“业务”能广义地解释为对组织的意图具有核心意义的活动。

5.2 方针

最高管理层应建立大数据安全方针，该方针应：

a) 与组织的意图相适宜；

b) 包括大数据安全目标(见 6.2)或为设定大数据安全目标提供框架；

c) 包括对满足适用的大数据安全相关要求的承诺；
d) 包括对持续改进大数据安全管理体系的承诺。

大数据安全方针应：

a) 形成文件化信息并可用；
b) 在组织内得到沟通；
c) 适当时，对相关方可用。

5.3 组织的角色、责任和权限

最高管理层应确保与大数据安全相关角色的责任和权限在组织内得到分配和沟通。

最高管理层应分配责任和权限，以便：

a) 确保大数据安全管理体系符合本文件的要求；
b) 向其报告大数据安全管理体系绩效。

6 规划

6.1 应对风险和机会的措施

6.1.1 通则

当规划大数据安全管理体系时，组织应明确 4.1 中提到的事项和 4.2 中提到的要求，并确定需要应对的风险和机会，以便：

a) 确保大数据安全管理体系能达到预期结果；
b) 预防或减少不良影响；
c) 达到持续改进。

组织应规划：

a) 应对这些风险和机会的措施；
b) 如何：
1)将这些措施整合到大数据安全管理体系过程中，并予以实现；
2) 评价这些措施的有效性。

6.1.2 大数据安全风险评估

组织应定义并应用大数据安全风险评估过程，以：

a) 建立并维护大数据安全风险准则，包括：
1) 风险接受准则；
2) 大数据安全风险评估实施准则。
b) 确保重复实施的大数据安全风险评估能产生一致的、有效的和可比较的结果。
c) 识别大数据安全风险：
1)应用大数据安全风险评估过程，以识别大数据安全管理体系范围内与信息保密性、完整性和可用性损失有关的风险；
2) 识别风险责任人。
d) 分析大数据安全风险：
1) 评估 6.1.2c)1) 中所识别的风险发生后，可能导致的潜在后果；
2)评估 6.1.2c)1) 中所识别的风险实际发生的可能性；
3) 确定风险级别。
e) 评价大数据安全风险：
1)将风险分析结果与 6.1.2a) 中建立的风险准则进行比较；
2) 对已分析的风险进行风险处置优先级排序。

组织应保留有关大数据安全风险评估过程的文件化信息。

6.1.3 大数据安全风险处置

组织应定义并应用大数据安全风险处置过程，以：

a) 在考虑风险评估结果的基础上，选择适合的大数据安全风险处置选项；

b) 确定实现已选的大数据安全风险处置选项所必需的所有控制；

注 1:组织能按需设计控制，或识别来自任何来源的控制。

c) 将 6.1.3b)确定的控制与附录 A 中的控制进行比较，并验证没有遗漏必要的控制；

d) 制定适用性声明，其包含：

——必要的控制(见 6.1.3b) 和 c)]；

——选择这些控制的合理性说明；

——必要的控制是否已实现；

——删减附录 A 中控制的合理性说明；

e) 制定正式的大数据安全风险处置计划；

f) 获得风险责任人对大数据安全风险处置计划的批准和对大数据安全残余风险的接受。

组织应保留有关大数据安全风险处置过程的文件化信息。

6.2 大数据安全目标及其实现规划

组织应在相关职能和层级上建立大数据安全目标。

大数据安全目标应：

a) 与大数据安全方针一致；

b) 可测量(如可行)；

c) 考虑适用的大数据安全要求，以及风险评估和风险处置的结果；

d) 得到监视；

e) 得到沟通；

f) 适当时予以更新；

g) 形成文件化信息且可用。

组织应保留有关大数据安全目标的文件化信息。

在规划如何达到大数据安全目标时，组织应确定：

a) 要做什么；

b) 需要什么资源；

c) 由谁负责；

d) 何时完成；

e) 如何评价结果。

6.3 针对变更的规划

当组织确定需要变更大数据安全管理体系时，应对这些变更的实施进行规划。

7 支持

7.1 资源

组织应确定并提供建立、实现、维护和持续改进大数据安全管理体系所需的资源。

7.2 能力

组织应：

a) 确定在其控制下工作且影响其大数据安全绩效的人员的必要能力；

b) 确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作；

c) 适用时，采取措施以获得必要的能力，并评估所采取措施的有效性；

d) 保留适当的文件化信息作为能力的证据。

注：适用的措施可能包括：例如，针对现有雇员提供培训、指导或重新分配工作；雇佣或签约有能力的人员。

7.3 意识

在组织控制下工作的人员应了解：

a) 大数据安全方针；

b) 其对大数据安全管理体系有效性的贡献，包括改进大数据安全绩效带来的益处；

c) 不符合大数据安全管理体系要求带来的影响。

7.4 沟通

组织应确定与大数据安全管理体系相关的内部和外部的沟通需求，包括：

a) 沟通什么；

b) 何时沟通；

c) 与谁沟通；

d) 如何沟通。

7.5 文件化信息

7.5.1 通则

组织的大数据安全管理体系应包括：

a) 本文件要求的文件化信息；

b) 组织所确定的、对于大数据安全管理体系有效性所必需的文件化信息。

注：不同组织有关大数据安全管理体系文件化信息的详略程度可能是不同的，这是由于：

1) 组织的规模及其活动、过程、产品和服务的类型；

2)过程及其相互作用的复杂性；

3) 人员的能力。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的：

a) 标识和描述(例如，标题、日期、作者或引用编号)；

b) 格式(例如，语言、软件版本、图表)和介质(例如，纸质的、电子的)；

c) 对适宜性和充分性的评审和批准。

7.5.3 文件化信息的控制

大数据安全管理体系及本文件所要求的文件化信息应得到控制，以确保其：

a) 在需要的地点和时间，是可用的和适宜使用的；

b) 得到充分的保护(例如，避免保密性损失、不恰当使用、完整性损失)。

为控制文件化信息，适用时，组织应开展以下活动：

c) 分发、访问、检索和使用；

注：访问可能隐含着仅允许浏览文件化信息，或允许并授权浏览和更改文件化信息等的决定。

d) 存储和保护，包括保持可读性；

e) 对变更的控制(例如，版本控制)；

f) 保留和处理。

组织确定的、为规划和运行大数据安全管理体系所必需的外来的文件化信息，应得到适当的识别，并予以控制。

8 运行

8.1 运行规划和控制

为了满足要求并实现第 6 章中确定的措施，组织应通过以下方式来规划、实现和控制所需的过程： ——建立过程的准则；

——根据准则实现对过程的控制。

文件化信息应可用，其程度足以确信这些过程按计划得到执行。

组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

组织应确保由外部提供的与大数据安全管理体系有关的过程是受控的。在数据生命周期中，组织可能参与数据形态的一个或多个阶段，将组织可能对数据实施的操作任务 的集合，即活动划分为：数据采集、数据存储、数据处理、数据分发以及数据删除等：

a) 数据采集。数据进入组织的大数据环境，数据可来源于其他组织或自身产生。

b) 数据存储。将数据持久存储在存储介质上。

c) 数据处理。通过该活动履行组织的职责或实现组织的目标。处理的数据可以是组织内部持久 保存的数据，也可以是直接接入分析平台的实时数据流。

d) 数据分发。组织在满足相关规定的情况下将数据处理生成的报告、分析结果等分发给公众或 其他组织，或将组织内部的数据适当处理后进行交换或交易等。

e) 数据删除。当组织决定不再使用特定数据时，组织可以删除该数据。

活动和活动之间可能存在数据流，组织应分析各活动中的安全风险，确保安全要求、策略和规程的 实施。

8.1.1 数据采集

8.1.1.1 数据采集活动的概念

数据采集活动的目标是获得数据，数据采集方式包括但不限于：

a) 网络数据采集。通过网络爬虫或公开API 等方式获取数据。

b) 从其他组织获取。通过线上或线下等方式从组织外获取数据。

c) 通过传感器获取。传感器包括温度传感器、电视、汽车、摄像头等公共和个人的智能设备。

d) 系统数据。组织内部的系统在运行过程中采集和产生的业务数据，以及各种系统、程序和服务运行产生的大量运维和日志数据等。

数据采集活动主要操作包括但不限于：发现数据源、传输数据、生成数据、缓存数据、创建元数据、数 据转换、数据完整性验证等。

8.1.1.2 安全要求

组织开展数据采集活动时，应：

a) 定义采集数据的目的和用途，明确数据采集源和采集数据范围；

b) 遵循合规原则，确保数据采集的合法性、正当性和必要性；

c) 遵循数据最小化原则，只采集满足业务所需的最少数据；

d) 遵循质量保障原则，制定数据质量保障的策略、规程和要求；

e) 遵循确保安全原则，对采集的数据进行分类分级标识，并对不同类和级别的数据实施相应的安 全管理策略和保障措施。对数据采集环境、设施和技术采取必要的安全管控措施。

8.1.2 数据存储

8.1.2.1 数据存储活动的概念

数据存储指将数据静态保存在大数据平台，存储的数据包括采集的数据、分析和处理的结果数据 等。存储系统可以是关系数据库、非关系数据库等，应支持对不同类型和格式的数据存储，且提供多种 数据访问接口，如文件系统接口、数据库接口等。直到数据被彻底删除之前，存储的数据均应由组织提 供恰当的安全保护。

组织应充分考虑使用第三方数据存储平台保存数据的安全风险。由于知识产权、法律法规等原因， 组织即使能对存储系统中的数据如个人信息或健康数据等进行有效控制，但可能不是数据的拥有者，组 织仍需承担数据的存储管理责任。

数据存储活动的主要操作包括但不限于：数据编解码、数据加解密、冷热数据分级存储、数据归档持 久存储、数据备份、数据更新、数据访问等。

8.1.2.2 安全要求

组织开展数据存储活动时，应：

a) 将不同类别和级别的数据分开存储，并采取物理或逻辑隔离机制。

b) 遵守确保安全原则，主要考虑以下几个方面：

1) 存储架构安全；
2) 逻辑存储安全；
3) 存储访问控制；
4) 数据副本安全；
5) 数据归档安全；
6) 数据时效性管理。

c) 建立数据存储冗余策略和管理制度，及数据备份与恢复操作过程规范。

8.1.3 数据处理

8.1.3.1 数据处理活动的概念

数据处理活动指通过数据分析和数据可视化等技术从数据中提取信息，提炼出有用知识和价值的 系列操作。

数据处理活动的主要操作包括但不限于：数据查询、数据读取、数据索引、批处理、交互式处理、流处 理、数据统计分析、数据预测分析、数据关联分析、数据可视化、生成分析报告等。

8.1.3.2 安全要求

组织开展数据处理活动时，应：

a) 依据个人信息和重要数据保护的法律法规要求，明确数据处理的目的和范围。

b) 建立数据处理的内部责任制度，保证分析处理和使用数据不超出声明的数据使用目的和范围。

c) 遵循最小授权原则，提供数据细粒度访问控制机制。

d) 遵循确保安全原则，主要考虑以下几个方面：

1) 分布式处理安全；
2) 数据分析安全；
3) 数据加密处理；
4) 数据脱敏处理；
5) 数据溯源。

e) 遵循可审计原则，记录和管理数据处理活动中的操作。

f) 对数据处理结果进行风险评估，避免处理结果中包含可恢复的敏感数据。

8.1.4 数据分发

8.1.4.1 数据分发活动的概念

数据分发活动指将原始数据、处理的数据等不同形式的数据传递给组织内部其他角色、外部实体或 公众等。数据分发包括线上或线下等多种方式。

数据分发的原因包括但不限于：

a) 组织内部部门间的数据交换；

b) 为外部生成报告，例如政府部门的统计数据；

c) 企业间的数据交换，为客户提供使用报告等；

d) 数据出售给其他组织；

e) 业务实现需求。

数据分发涉及的主要操作包括但不限于：数据传输、数据导出、数据交换、数据交易、数据共享等。

8.1.4.2 安全要求

组织开展数据分发活动时，应：

a) 遵循责任不随数据转移原则。

b) 个人信息、重要数据等有处境需求时，应根据相关法律法规、政策文件盒标准执行处境安全 评估。

c) 在数据分发前，对数据进行风险评估，确保数据分发后的风险可承受，并通过合同明确数据接收方的数据保护责任。

d) 在数据分发前，对数据的敏感性进行评估，根据评估结果对需要分发的敏感信息进行脱敏 操作。

e) 遵循可审计原则，记录时间、分发数据、数据接收方等相关信息。

f) 评估数据分发中的传输安全风险，确保数据传输安全。

g) 提供有效的数据安全共享机制。

h) 建立数据发布的审核制度，严格审核发布信息符合相关法律法规要求。明确数据发布的内容 和范围。对发布的数据开展定期审核。

8.1.5 数据删除

8.1.5.1 数据删除活动的概念

数据删除活动指组织删除自有或租用的大数据平台上的数据及其副本。如果数据来自外部实时数 据流，还应断开与实时数据流的链接。

数据被删除的原因包括但不限于：

a) 为了减少数据泄露的风险。避免数据被不适当的分发或处理。

b) 删除不相关或不正确的数据。数据与最初使用目的不再相关，或数据不正确。

c) 业务完成后的数据删除处理。数据业务完成服务目标，不再需要保存相关数据。

d) 满足客户的数据删除要求。法律法规要求保留的数据除外。

数据删除活动的主要操作包括但不限于：删除元数据、删除原始数据及其副本、断开与外部实时数 据流的链接、删除数据的访问接口、不可恢复的数据销毁等。

8.1.5.2 安全要求

组织开展数据删除活动时，应：

a) 删除超出数据留存期限的相关数据，对留存期限有明确规定的，按相关规定执行；

b) 依照数据分类分级建立相应的数据删除机制，明确需要进行数据销毁的数据、方式和要求，明 确销毁数据范围和流程；

c) 遵守可审计原则，建立数据删除策略和管理制度，记录数据删除的操作时间、操作人、操作方 式、数据内容等相关信息。

8.2 大数据安全风险评估

组织参照 GB/T 20984—2007 开展风险评估工作，并关注大数据环境下安全风险评估的特点。附 录B 是生命科学大数据风险分析示例，附录C 列出了大数据面临的一些安全风险。

8.2.1 资产识别

组织开展资产识别时，应关注大数据的资产特点，包括但不限于：

a) 个人信息；
b) 重要数据；
c) 大数据可视化算法与软件；
d) 大数据分析算法与软件；
e) 大数据处理框架，如流处理框架、交互式处理框架、离线处理框架；
f) 大数据存储框架，如分布式文件系统、非关系型数据库等；
g) 大数据平台计算资源(如 CPU、内存、网络等)管理框架等。

8.2.2 威胁识别

组织开展威胁识别时，应关注大数据环境下的威胁特点，包括但不限于：

a) 潜在的不利因素：
——潜在攻击方具有的资源、技术能力、动机等，常见的攻击方有个人、组织、国家等；
——潜在攻击方窃取、利用和滥用数据的意图；
——大数据访问、存储和处理所需资源；
——直接访问数据或窃取数据的风险；
——发起攻击、恶意利用大数据的成本与收益。
b) 恶意利用所需的科学专业知识和技能：
——数据和结果分析需要使用的技能、专业知识；
——数据使用和结果分析需要的技术和设备；
——利用系统脆弱性需要的技能、技术和知识。
c) 数据出境威胁。

8.2.3 脆弱性识别

组织开展脆弱性识别时，应关注大数据环境下的脆弱性特定，包括但不限于：

a) 大数据存储、处理等基础软件和基础设施的脆弱性；
b) 大数据相关系统的脆弱性。

8.2.4 已有安全措施确认

组织应对已采取的安全措施的有效性进行确认。安全措施的选择可以参考 GB/T 35274—2017。

8.2.5 风险分析

组织应采用适当的方法与工具确定威胁利用脆弱性导致大数据安全事件发生的可能性，综合安全 事件所作用的大数据资产价值及脆弱性的严重程度，判定安全事件造成的损失对国家安全、社会公共利 益、组织和个人利益的影响。

8.3 大数据安全风险处置

组织应实现大数据安全风险处置计划。

组织应保留大数据安全风险处置结果的文件化信息。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

a) 需要被监视和测量的内容，包括大数据安全过程和控制；

b) 适用的监视、测量、分析和评价的方法，以确保得到有效的结果。所选的方法宜产生可比较和 可再现的结果，才会被视为有效；

c) 何时执行监视和测量；

d) 谁监视和测量；

e) 何时分析和评价监视和测量的结果；

f) 谁分析和评价这些结果。

作为结果证据的文件化信息应可用。

组织应评价大数据安全绩效和大数据安全管理体系的有效性。

9.2 内部审核

9.2.1 通则

组织应按计划的时间间隔进行内部审核，以提供下列相关信息：

a) 大数据安全管理体系是否符合：

1)组织自身对大数据安全管理体系的要求；

2)本文件的要求；

b) 大数据安全管理体系是否得到有效实现和维护。

9.2.2 内部审核方案

组织应规划、建立、实施和维护审核方案(一个或多个),包括审核频次、方法、责任、规划要求和 报告。

组织应根据相关过程的重要性和以往审核的结果，建立审核方案。

组织应：

a) 定义每次审核的审核准则和范围；

b) 选择审核员并实施审核，确保审核过程的客观性和公正性；

c) 确保将审核结果报告至相关管理层。

作为审核方案实施和审核结果证据的文件化信息应可用。

9.3 管理评审

9.3.1 通则

最高管理层应按计划的时间间隔评审组织的大数据安全管理体系，以确保其持续的适宜性、充分性和 有效性。

9.3.2 管理评审的输入

管理评审应包括下列相关信息。

a) 以往管理评审提出的措施的状态。

b) 与大数据安全管理体系相关的外部和内部事项的变化。

c) 大数据安全管理体系相关方的需求和期望的变化。

d) 有关大数据安全绩效的反馈，包括以下方面的趋势：

1)不符合与纠正措施；

2) 监视和测量结果；

3) 审核结果；

4) 大数据安全目标完成情况。

e) 相关方反馈。

f) 风险评估结果及风险处置计划的状态。
g) 持续改进的机会。

9.3.3 管理评审的结果

管理评审的结果应包括与持续改进机会相关的决定以及变更大数据安全管理体系的任何需求。
作为管理评审结果证据的文件化信息应可用。

10 改进

10.1 持续改进

组织应持续改进大数据安全管理体系的适宜性、充分性和有效性。

10.2 不符合与纠正措施

当发生不符合时，组织应：
a) 对不符合做出反应，且适用时：

1) 采取措施，对其予以控制和纠正；
2) 处理其后果；

b) 通过以下活动，评价采取消除不符合原因的措施的需求，以防止不符合再次发生或在其他地方发生：

1) 评审不符合；
2) 确定不符合的原因；
3) 确定类似的不符合是否存在，或是否可能发生；

c) 实现任何需要的措施；
d) 评审任何所采取的纠正措施的有效性；
e) 必要时，对大数据安全管理体系进行变更。

纠正措施应与所发生的不符合的影响相适应。
作为以下证据的文件化信息应可用：
a) 不符合的性质及所采取的任何后续措施；
b) 任何纠正措施的结果。