ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 35274—2023
代替 GB/T 35274—2017

数据安全技术
大数据服务安全能力要求

Data security technology—
Security capability requirements for big data services

2023-08-06 发布　　2024-03-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件代替GB/T 35274—2017《信息安全技术　大数据服务安全能力要求》，与GB/T 35274—2017相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了数据生命周期、数据服务、数据交换、数据共享和重要数据（见2017年版的第3章）5个术语和定义，增加了数据处理、数据安全、数据保护、数据收集、数据存储、数据使用、数据加工、数据传输、数据提供、数据公开和数据销毁（见第3章）11个术语和定义，修改了大数据平台、大数据应用、大数据系统、大数据使用者、大数据服务、大数据服务提供者和数据供应链（见第3章，2017年版的第3章）7个术语和定义的描述；

b) 删除了总体要求（见2017年版的4.1）和要求分级（见2017年版的4.2），对标准整体内容进行了梳理（见第4章，2017年版的4.3）；

c) 删除了服务规划与管理（见2017年版的5.4）、数据供应链管理（见2017年版的5.5）和合规性管理（见2017年版的5.6），修改了策略与规程、组织和人员以及资产管理安全能力要求（见5.1、5.2、5.3，2017年版的5.1、5.3、5.2）；

d) 重组并更改了数据采集、数据传输、数据存储、数据处理、数据交换和数据销毁的数据活动安全要求，按照数据安全法和个人信息保护法要求的数据收集、存储、使用、加工、传输、提供、公开和销毁的数据处理过程明确了大数据服务提供者的大数据处理安全能力要求（见第6章，2017年版的第6章）；

e) 增加了“大数据服务安全风险管理能力”，从风险识别、安全防护、安全监测、安全检查、安全响应和安全恢复环节，规定了大数据服务提供者在大数据系统运营中的数据安全风险管理能力（见第7章）；

f) 删除了附录A中（见2017年版的附录A）。

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。

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：清华大学、北京大学、中国电子技术标准化研究院、中国网络安全审查技术与认证中心、中国信息安全测评中心、国家计算机网络应急技术处理协调中心、深信服科技股份有限公司、浙江蚂蚁小微金融服务集团有限公司、北京快手科技有限公司、阿里巴巴（中国）有限公司、腾讯云计算（北京）有限责任公司、中国科学院信息工程研究所、华控清交信息科技（北京）有限公司、北京天融信网络安全技术有限公司、北京火山引擎科技有限公司、长扬科技（北京）股份有限公司、上海观安信息技术股份有限公司、华为技术有限公司、北京奇虎科技有限公司、启明星辰信息技术集团股份有限公司、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、北京数安行科技有限公司、上海赛源科技服务有限公司、杭州世平信息科技有限公司、北京信安世纪科技股份有限公司、联想（北京）有限公司、杭州安恒信息技术股份有限公司、成都卫士通信息产业股份有限公司、上海三零卫士信息安全有限公司、陕西省信息化工程研究院、上海商汤智能科技有限公司、北京神州绿盟科技有限公司、北京百度网讯科技有限公司、浙江大华技术股份有限公司、北京腾云天下科技有限公司。

本文件主要起草人：叶晓俊、谢安明、吴迪、王建民、赵英华、徐羽佳、刘贤刚、陈兴蜀、赵芸伟、宋博韬、白晓媛、落红卫、陈驰、靳晨、叶润国、陈星、查海平、谢江、刘玉红、李娇娇、张亚京、兰安娜、李世奇、胡影、金涛、闵京华、王永霞、葛小宇、张屹、都婧、周润松、陈洪运、杨保磊、丁国徽、吴高、望娅露、

徐浩、王海棠、张宇、马红霞、刘玉岭、王庆磊、瓮辉辉、潘正泰、葛梦莹。

本文件及其所代替文件的历次版本发布情况为：

——2017 年首次发布为 GB/T 35274—2017；

——本次为第一次修订。

数据安全技术
大数据服务安全能力要求

1 范围

本文件规定了大数据服务提供者的大数据服务安全能力要求，包括大数据组织管理安全能力、大数据处理安全能力和大数据服务安全风险管理能力的要求。

本文件适用于指导大数据服务提供者的大数据服务安全能力建设，也适用于第三方机构对大数据服务提供者的大数据服务安全能力进行评估。

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 5271(所有部分) 信息技术 词汇

GB/T 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 35295—2017 信息技术 大数据 术语

3 术语和定义

GB/T 5271(所有部分)、GB/T 25069—2022、GB/T 35273—2020 和 GB/T 35295—2017 界定的以及下列术语和定义适用于本文件。

3.1

大数据 big data

具有体量巨大、来源多样、生成极快、宜多变等特征，并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

[来源：GB/T 35295—2017，2.1.1]

3.2

数据处理 data handling

数据操作的系统执行，以实现特定目的的数据收集、存储、使用、加工、传输、提供、公开、销毁等活动。

注：数据操作如数据的数学运算或逻辑运算，数据的归并或分类，文本的操作、存储、检索、显示或打印，数据的挖掘分析、数据可视化等。

[来源：GB/T 5271.1—2000，01.01.06，有修改]

3.3

数据收集 data collection

根据特定的目的和要求，从一种或多种数据源选择和获取数据，并对数据进行清洗、标识、加载等数

据操作，形成数据资产的数据处理活动。

3.4

数据存储　data storage

将数据持久化保存在硬盘等存储介质中的数据处理活动。

3.5

数据使用　data usage

依据数据权属及收集和使用数据的目的和范围，以及确定的授权和访问控制策略，控制组织、人员或信息系统等主体对数据资产进行读取、检索、展示等操作的数据处理活动。

注：数据使用需对数据的种类、范围、处理方式及其目的等进行相应的控制，包括数据使用前条件控制和数据使用后义务履行。使用前条件是访问控制引擎在授权过程中，允许主体访问或使用客体数据前需核验的决策因素集。条件控制是用来检查存在的约束限制，数据权属及使用权限是否有效，哪些约束限制需更新等。使用后义务履行是主体在获得对客体的数据使用权限后要执行的要求。主体在获得权限执行数据使用操作后有执行获取这些权限的义务责任。

3.6

数据加工　data processing

通过数据变换、数据转换、数据编码、数据计算、数据压缩、数据分析等数据操作，生成新数据（集）的数据处理活动。

注：数据加工一般会涉及数据自身的改变，需要先读取数据，并经过变换、转换、纠错、编码、分析、挖掘、脱敏等数据操作生成新数据（集）。

3.7

数据传输　data transmission

通过信息通信设备将数据从一个网络节点传送到一个或多个网络节点的数据处理活动。

注：网络节点可以是计算机、程序、终端设备、存储器、信息系统等。

[来源：GB/T 5271.9—2001，09.01.02，有修改]

3.8

数据提供　data provision

向组织内其他责任主体或其他组织提供所控制的数据资产的数据处理活动。

注：组织内数据提供一般指跨安全域的数据交换、数据共享、数据转让等数据操作，跨组织的数据提供还可涉及数据的权益归属、数据跨境安全评估以及个人信息保护影响评估等数据操作。

3.9

数据公开　data disclosure

向其他组织、个人或指定范围公开所控制的数据资产的数据处理活动，使其可合规地获取所公开的数据。

3.10

数据销毁　data destruction

抹去或覆盖存储介质中的数据或销毁存储介质的数据处理活动。

注：数据销毁分为数据删除和介质销毁两种。数据删除是指在所涉及的信息系统及数据存储设备中抹去数据或者覆盖存储的数据，使其不可被检索、访问的状态；介质销毁则采用物理破坏、化学腐蚀等方法直接销毁存储数据的介质，以达到彻底删除数据的目的。

3.11

大数据平台　big data platform

采用分布式存储和计算技术，提供大数据处理功能，支持大数据应用安全高效运行的软硬件集

合，包括监视数据输入/输出、控制数据处理活动等软硬件基础设施及其所控制的数据资产。

注：平台指由一组子系统和技术形成的软硬件设施组成，通过一些接口和使用工具提供一组一致的功能，任何由它所支持的应用都可以使用平台的功能而不必关心其实现细节。

3.12

大数据应用　big data application

由大数据平台支撑，执行数据处理活动，提供大数据服务的应用系统。

3.13

大数据系统　big data system

包括大数据平台、大数据应用及其所需和控制数据资产的信息系统。

3.14

大数据服务　big data service

利用大数据技术开展数据处理，并通过底层大数据平台和上层多种大数据应用以服务方式为大数据使用者提供有价值的数据处理功能的活动。

注：大数据服务封装了大数据使用者所需的数据处理活动，且采用标准化协议来识别、注册和发布相关的数据服务，以便使大数据服务提供者以信息服务的方式交付价值给大数据使用者。

3.15

大数据使用者　big data user

使用大数据系统的末端个人、组织及其他信息系统或智能终端设备。

3.16

大数据服务提供者　big data service provider

拥有大数据系统，提供大数据服务的组织。

注：大数据服务提供者是一种拥有或可获得大数据服务所需数据资产的网络运营者。

3.17

数据安全　data security

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。

注：GB/T 5271.8—2001 的术语 08.01.04 定义数据安全为“适用于数据保护的计算机安全”。

3.18

数据保护　data protection

实施适当的管理、技术或物理手段，以防止未授权的有意或无意地泄露、修改或破坏数据的活动。

[来源：GB/T 5271.8—2001，08.06.02，有修改]

3.19

数据供应链　data supply chain

在大数据服务中，数据处理涉及数据需求及供应关系目的的上游与下游组织的数据资源及数据操作所形成的链接集。

注：数据供应链管控的目标是使大数据服务提供者能在正确的时间，将大数据服务所需的各种数据资源，通过计划、协调、操作、控制、优化等活动，按照正确的服务协议供应给大数据使用者。

4　概述

本文件面向有大数据平台、大数据应用和大数据服务所需数据资源的组织，从大数据组织管理安全能力、大数据处理安全能力和大数据服务安全风险管理能力三个方面规定了大数据服务提供者的大数

据服务安全能力要求，其中：

a) 大数据组织管理安全能力：按照信息安全管理体系要求制定大数据安全策略与规程，从大数据服务组织与人员的安全管理，以及大数据服务所需的数据资产与系统资产管理视角制定数据安全管理等制度，满足大数据服务组织管理安全合规及数据安全风险管控要求；

b) 大数据处理安全能力：针对数据收集、存储、使用、加工、传输、提供、公开、销毁等数据处理活动，从大数据平台和大数据应用业务及技术层面采取数据保护措施，满足大数据服务中数据处理活动相关的数据保护要求；

c) 大数据服务安全风险管理能力：按照大数据服务中数据业务流转过程和数据处理活动安全保护要求，从风险识别、安全防护、安全监测、安全检查、安全响应和安全恢复六个环节建立大数据服务安全风险管理能力，采取风险应对措施使大数据服务及其数据资产始终处于有效保护、合法利用状态，保障大数据系统运营者所提供的大数据服务的可持续性。

大数据服务提供者依据被保护数据资产和系统资产的重要性，以及大数据系统遭受破坏可能导致的危害程度，结合自身的大数据服务业务、大数据服务目标和支撑大数据服务的软硬件设施、大数据平台与大数据应用功能，参考本文件进行大数据组织管理安全能力、大数据处理安全能力和大数据服务安全风险管理能力的建设和评估（涉及重要数据和核心数据处理活动的，需依据相关法律法规规定和主管部门制定的相关管理制度，对数据安全风险管理能力进行建设和评估），满足大数据服务中数据处理活动合规性、数据服务连续性和数据服务风险可控性的要求。

5 大数据组织管理安全能力

5.1 策略与规程

要求包括：

a) 应明确数据处理的安全方针、目标和原则，制定网络安全和数据安全等管理制度，并将其分发至数据处理活动相关工作的职能部门、岗位和人员；

b) 应制定组织开展数据处理活动的数据安全策略与规程，内容包括数据处理目的、范围、方式、岗位、责任及合规性要求等；

c) 应建立数据供应链安全管控规程，以书面协议等方式与数据供应链涉及上下游组织明确约定交换共享数据的使用目的、范围、数量、供应方式、安全责任与义务、保密要求等内容，在涉及重要数据和敏感个人信息时，宜包括大数据服务相关网络产品和服务筛选机制、筛选指标和评价方法的约定；

d) 应制定与数据安全管理制度、数据安全策略与规程、数据供应链安全管控规程相匹配的大数据平台和大数据应用安全技术机制与措施的实施细则；

e) 应建立数据安全风险评估和个人信息保护影响评估规程，制定应对数据安全和个人信息保护的实施细则和操作规范，包括依据国家相关规定向主管部门报送安全风险评估报告的制度；

f) 应建立数据安全和个人信息保护投诉、举报渠道及受理处置规程，公布接受投诉、举报的联系方式等信息，及时受理、处置关于数据安全和个人信息保护的投诉举报，对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益，必要时公开披露收到的投诉、受理进度以及最终处理结果，接受社会监督；

g) 应在组织架构发生重大调整或大数据服务业务发生重大变化时，或因合并、分立、解散、被宣告破产等原因需要转移数据时，及时评估数据安全管理制度、数据安全策略与规程及数据供应链安全管控规程的适用性，并根据评估结果修订数据安全管理制度、数据安全策略和规程及数据

供应链安全管控规程；

h) 应对组织数据安全管理制度、数据安全策略和规程、大数据平台和应用的数据保护措施等进行持续改进，如以定期通过信息安全管理体系认证、网络安全等级保护测评、数据安全风险评估等方式明确大数据服务安全能力持续提升计划和实施机制；

i) 应建立落实数据安全和个人信息保护法律法规及相关数据安全保护的责任考核制度，涉及敏感个人信息处理、重要数据出境等应依据合规性要求做出安全责任的承诺；

j) 应建立机器可读的数据安全策略与规程履行机制，对大数据服务过程中涉及的角色管理、访问控制、安全审计、资源调配、服务跟踪等策略与规程实施过程进行记录与归档；宜实现自动化的大数据服务策略与规程的执行情况的跟踪、合规审核和服务违法行为的追溯。

5.2 组织与人员

5.2.1 组织职责

要求包括：

a) 应明确数据安全负责人，负责组织日常的数据安全管理工作；涉及重要数据的组织应成立数据安全管理机构，组织最高管理人员或高级管理人员宜作为组织数据安全负责人，并配备专职的数据安全管理人员和技术人员；

b) 应明确大数据系统规划、建设和使用相关的工作职能部门，制定各部门网络安全责任清单及追责制度，使大数据系统运营安全风险可控和大数据服务业务可持续；

c) 应明确数据安全风险评估、数据安全应急处置等工作的职能部门，明确工作职责；

d) 应建立有效宣贯机制，使得组织所有人了解数据安全工作重要性及相关部门职责；

e) 应建立有效汇报和沟通机制，保证数据安全事件等安全风险信息能及时汇报给相关职能部门；

f) 应建立监督考核机制，落实执行对数据安全管理工作的监督检查和考核制度，定期对数据安全工作相关部门进行安全责任评估。

5.2.2 岗位职责

要求包括：

a) 应围绕数据采集、存储、加工、使用、提供、公开等处理活动设置相应的数据操作岗位，明确岗位的安全职责，涉及重要数据的组织应设立专职的数据安全管理岗位；

b) 应列出重要岗位清单，包括能处理大量数据、处理重要数据或处理敏感个人信息等操作的岗位，明确重要岗位的职责和安全责任；

c) 应建立岗位职责检查机制，定期检查岗位间分离相冲突的责任及职责范围，以降低未授权或无意识的修改或者不当使用数据的机会；

d) 应按照大数据技术架构和大数据服务业务安全建立大数据用户授权策略和访问控制模型，明确不同岗位或用户角色的访问机制安全要求；

e) 宜基于用户访问控制模型建立灵活、实用的授权管理机制，如基于角色的权限分配管理机制或基于上下文的动态授权管理机制。

5.2.3 人员管理

要求包括：

a) 应制定大数据服务人力资源管理安全策略，明确不同职能部门和安全岗位人员的权责和能力等要求；

b) 应制定人员招聘、录用、培训、考核、选拔、上岗、调岗、离岗等环节中大数据服务人员安全管理的操作规程；
c) 应明确重要岗位的人员能力要求，确定相应的考核内容与考核指标，进行必要的背景调查和签署保密协议；
d) 应建立人员数据安全责任管理机制，在其调离或终止劳动合同时将其所拥有的角色和责任移交给新的责任人员，并按照制度规范对造成数据安全风险的人员追责，记录人员责任信息；
e) 应建立第三方人员安全管理制度，并按照数据处理安全合规性要求签署保密协议，定期对第三方人员规范性行为进行安全审查；
f) 应与所有涉及大数据服务岗位人员签订安全责任协议，人员调离或终止劳动合同时归还组织的软硬件资产，及时变更岗位变动人员的数据处理权限，终止离岗人员的所有数据处理权限。

5.2.4 培训管理

要求包括：
a) 应制定数据开发利用和数据安全保护相关的教育培训计划，每年组织开展全员数据安全教育培训，并依据培训反馈效果定期对教育培训计划进行审核和更新；
b) 应按计划采取多种方式培养数据开发利用人员和数据安全专业人员，培训内容可包括法规、政策、标准、技术、能力、安全意识等，并对培训结果进行考核、记录和归档；
c) 应制定重要数据、敏感个人信息等数据处理活动重要岗位的上岗、转岗、晋升等相应的人员安全能力要求的教育培训计划，并对培训计划、培养方式、培训内容定期审核和更新；
d) 应针对涉及重要数据、敏感个人信息处理等重要岗位的人员，开展大数据服务安全操作技能培训与培训效果实践考核。

5.3 资产管理

5.3.1 数据资产

要求包括：
a) 应建立数据资产安全管理规范，明确数据资产的安全管理目标和原则；
b) 应建立数据分类分级策略，明确数据分类分级的制度和操作规程，以及数据分类分级的变更审批流程和机制；
c) 应建立数据资产清单，明确大数据服务相关的数据资产的业务基础属性、类别、级别及相关方的责任、义务与权利等安全属性；
d) 应建立安全属性标记策略、标记定义和标记变更控制制度与操作规程，宜具备数据资产安全属性自动标记能力；
e) 应建立数据资产操作审计机制，实现数据资产管理操作行为的可审计和可追溯；
f) 应建立数据资产管理平台，制定数据资源整合操作规程，实现对数据资产的数字化管理；
g) 应定期审核和更新数据资产安全管理相关的分类分级策略、操作规程及其数据资产清单等。

5.3.2 系统资产

要求包括：
a) 应建立系统资产安全管理规范，明确系统资产安全管理目标和原则；
b) 应建立系统资产建设和运营管控措施，明确规划、设计、采购、开发、运行、维护及报废等系统资产管理过程的安全要求，包括内外部人员在任职期内领用和归还系统资产以及在终止任用、合

同或协议时归还所使用系统资产的管理制度和机制；

c) 应建立系统资产登记制度，形成系统资产清单，明确系统资产安全责任主体及相关方权责清单，并定期审核和更新系统资产管理相关的运营管控措施、资产登记制度和系统资产清单等；

d) 应建立系统资产分类和标记规程，使资产标记易于填写并清晰关联到对应系统资产上；

e) 应通过系统资产管理的自动化手段，对系统资产进行注册、使用、状态监控进行数字化管理，具备对系统资产清单、系统访问权限清单等进行持续更新的能力。

6 大数据处理安全能力

6.1 数据收集

6.1.1 数据获取

要求包括：

a) 应制定数据获取操作规程，明确数据收集的数据源、获取目的，规范数据获取渠道及其获取数据格式、获取流程和获取方式，并定期评估数据获取操作规程的合规性；

b) 应评估数据获取环境、设施和技术工具对数据提供者的网络服务的性能、功能带来的影响，使数据获取过程不干扰数据提供者的网络服务可用性；

c) 应采取技术和管理措施，使数据获取相关工具在获得授权后才能收集数据；宜具备对超出法律法规规定和合同约定规模、范围获取数据的异常行为进行检测告警能力；

d) 应对涉及个人信息等数据获取场景具备针对潜在数据泄露风险的技术防范措施；

e) 应在获取重要数据和敏感个人信息时，与数据提供方通过签署协议、承诺书等方式，明确双方法律责任及数据安全保护责任和义务；

f) 应跟踪和记录数据获取操作过程，具备针对数据获取操作过程的追溯能力；

g) 应在发现可能违反法律法规，或者侵犯他人知识产权等合法权益时，立即停止获取数据操作并采取相应的补救措施。

6.1.2 数据清洗

要求包括：

a) 应制定数据变换、转换、去重、纠错等数据清洗操作规程，明确数据清洗操作的要求、规则和方法，使数据清洗操作前后数据间的映射关系不变；

b) 应采取技术手段和管理措施对所获取或清洗操作生成的数据进行保护，包括但不限于衍生数据以及操作日志保护等；

c) 应记录数据清洗操作行为，在数据清洗完成后对产生的中间或临时数据进行安全删除。

6.1.3 数据标识

要求包括：

a) 应依照数据分类分级要求建立数据识别和标记的操作规程；

b) 应采用技术措施对收集的数据进行识别，并依据数据分类分级策略对收集数据的安全属性进行标记；

c) 应定期对数据识别和标记的效果、影响范围等数据安全风险进行评估，宜通过工具对数据的标识、审核及标记结果使用过程进行管理，实现数据识别和标记变更的可追溯。

6.1.4 数据加载

要求包括：

a) 应综合数据规模、增长速度、业务需求、数据加载有效性等因素制定跨安全域的不同数据源数据加载的操作规程，明确数据安全加载的要求、规则和方法；

b) 应具备对数据加载终端或加载服务组件等进行身份鉴别的能力；宜采取多因素身份鉴别技术，满足数据加载操作人员身份的真实性和访问权限的合法性要求；

c) 应记录数据加载操作过程，在数据加载完成后对数据加载通道缓存的数据进行安全删除；

d) 应提供数据加载通道的冗余备份、加载接口的流量过载监控等数据安全可靠加载的安全措施。

6.2 数据存储

6.2.1 存储架构

要求包括：

a) 应建立可伸缩的数据存储架构，提供存储模块的装载与可卸载的扩展存储空间管理功能，满足大数据平台管控数据资源可持续增长的扩展存储需求；

b) 应制定数据存储架构安全管控规则，包括外部身份鉴别与访问控制规则、存储数据转移安全规则、存储数据完整性和多副本数据一致性的管理规则等；

c) 应建立数据逻辑存储安全管理操作规范，具备对数据分片和数据分布式存储等逻辑存储结构的分层和分级保护能力，满足不同数据类型、不同数据容量、不同业务需求和不同数据用户的逻辑存储安全管理要求；

d) 应提供技术措施使数据存储架构具备满足不同技术架构层次的加密存储的能力；

e) 应选择适当的使数据存储架构实现容灾备份的能力；宜提供数据存储本地和异地的容灾备份的基础设施能力；

f) 应具备依据访问频率和数据时效性高低设计的数据分层存储管理机制与技术，支持数据在各分层间的自动迁移，提升数据存储和访问效率；

g) 应提供数据分离存储、分布式存储等降低数据安全风险的方法及技术机制，涉及在境内收集和产生的重要数据和个人信息存储应符合法律法规要求。

6.2.2 数据副本与备份

要求包括：

a) 应建立数据存储冗余策略和数据复制、备份和恢复机制相关数据副本的操作规范，包括副本数量、访问权限管理、数据同城备份与异地容灾备份方案与机制等；

b) 应建立数据副本的强一致性、弱一致性等控制策略与操作规范，满足数据不同一致性级别的数据复制等数据副本存储管理要求；

c) 应建立数据副本的定期检查和更新程序，包括数据副本更新频率、保存期限等，定期对数据副本和备份数据的一致性进行检测验证，保证数据副本和备份数据的有效性；

d) 应对复制、备份等操作生成的数据副本执行和数据源同样的安全管控措施，包括身份鉴别、访问控制、完整性校验等技术机制；

e) 应建立数据复制、备份和恢复操作的日志记录规范，记录数据复制、备份和恢复等数据副本操作过程，实现数据副本和备份数据管理过程可溯源；

f) 应提供数据副本和备份数据存储的多种压缩实现技术机制。

6.2.3 数据归档

要求包括：

a) 应依据数据资产的重要性和大数据业务连续性等需求，建立数据归档存储相关的操作规程；
b) 应建立数据分层归档架构，支持大数据服务中各种场景的海量数据的有效归档、恢复和使用；
c) 应建立归档数据的存储安全策略和管控措施，保证非授权用户不能访问归档数据；
d) 应建立归档数据的压缩或加密策略，使归档数据存储空间的有效安全利用；
e) 应建立归档数据安全管理制度，定期采取技术手段和管控措施验证归档数据的完整性和可用性，指定专人负责归档数据的安全管理。

6.2.4 数据留存

要求包括：

a) 应建立数据存储时效性管控措施和操作规程，按照法律法规和主管部门的数据保存时长要求对相关数据进行留存；
b) 应具备数据存储和授权时效性与数据留存时长的管理和控制能力；
c) 应建立对存储数据、相关备份、复制与归档数据副本的安全删除方法和技术机制，限期删除已完成数据处理目的和达到存储期限的数据；
d) 因收购、兼并、重组、委托处理、破产或其他合同等因素，导致其数据服务转让或终止，应保证其备份、复制或归档的冗余数据，包括操作日志等衍生数据的留存时长符合相关规定。

6.2.5 密钥管理

要求包括：

a) 应建立数据存储架构的密钥管理操作规范，对密钥的产生、分发、存储、使用、更新、归档、备份、恢复和销毁等密钥操作管理进行记录；宜具备密钥集成管理能力，提供支持密文数据透明处理等密钥使用的应用接口；
b) 应提供支持商用密码算法集成的密钥管理互操作性接口，宜建立多层存储加密及密钥管理的技术架构，满足大数据系统的不同层次的接口调用或应用透明的存储加密需求。

6.2.6 多租户数据存储

要求包括：

a) 应制定多租户数据存储隔离操作规程，包括租户应用上线、下线的数据迁移操作规程；
b) 应建立多租户数据安全存储技术机制，提供数据分割、存储区切割等技术机制来隔离多租户数据资源；宜依据不同租户空间内的用户需求，提供用户定制化的租户数据安全保护技术机制；
c) 应建立多租户数据复制、备份、归档等存储冗余信息保护技术机制与操作规范；
d) 应建立多租户数据可用性保障策略和技术机制，包括但不限于故障转移、多副本自动管理等。

6.3 数据使用

6.3.1 合规管理

要求包括：

a) 应明确数据责任主体、数据主体、数据控制者或数据处理者及其相关参与者的责任、义务与权利约束和限制条件，使数据的使用不能损害相关权利人的合法权益；

b) 应明确数据使用确权授权机制，建立数据使用授权管理操作规范与技术机制，包括多层次主动防御机制和数据保护措施的授权管理方法；
c) 应建立数据使用审计记录和受保护的数据使用日志的分布式存储机制和管控措施，具备对潜在违约数据使用者的责任识别和处置能力；
d) 应建立收集和汇聚数据的授权管理机制，包括在合法正当、知情同意等原则基础上确定的原始数据收集目的、用途等权限，和数据控制者对汇聚数据资产的控制权限等；
e) 宜具备对数据使用的违约行为、缔约过失行为、侵权行为等进行分析预警的能力和发生数据使用风险后的应对处置能力。

6.3.2 访问控制

要求包括：

a) 应综合主体角色与安全级别、数据分类分级与业务需要、数据使用时效性等因素，采用访问控制机制，依据大数据技术架构实施大数据使用者身份标识与鉴别、存储数据访问授权等策略，实现存储数据使用相关的访问授权；
b) 应利用大数据系统的分布式层次访问控制技术实施大数据使用者身份标识与鉴别、存储数据访问控制等策略，并提供集成外部存储数据资源的访问控制的接口；
c) 应建立面向大数据系统应用层、平台层、数据存储层等不同技术层次的数据访问接口、管理工具和管理命令的管控措施和技术机制，包括访问控制时效的管理和验证、应用接入数据存储操作的有效性取证机制等；
d) 应建立访问控制管控操作日志记录及其审计日志数据的分布式存储机制，具备对数据使用和访问操作进行记录、管理、安全审计和事件归因等能力。

6.3.3 数据展示

要求包括：

a) 应建立数据展示操作规范，对数据的展示范围、内容、方式等进行安全评估，确定数据展示的必要性和安全性；宜具备根据大数据使用者角色及授予的权限在大数据技术架构不同层次自动展示相应数据类型和安全级别数据的能力；
b) 应在展示重要数据和敏感个人信息时，采用数据脱敏等技术，并通过防截屏、防复制、限制打印、屏幕水印等控制措施，降低数据展示时的数据泄露风险；
c) 应在数据展示完成后，及时安全删除本地缓存或展示通道缓存中的数据，包括数据展示操作产生的中间或临时数据。

6.4 数据加工

6.4.1 分布式计算

要求包括：

a) 应建立分布式计算节点间安全连接策略和互操作规范，采用节点认证等技术机制保证大数据服务处理节点接入身份的真实性；
b) 应建立分布式计算节点和用户安全属性的周期性确认机制，保证预定义分布式计算安全策略存储和数据加工相关算法在各节点实施技术机制的一致性；
c) 应建立分布式计算过程中数据文件鉴别、用户身份鉴别等主客体鉴别的技术机制，保证分布式计算数据和主体行为的真实性；

d) 应建立分布式计算过程中不同节点的数据副本的更新检测机制，保证数据副本的完整性和一致性；

e) 应建立分布式计算中数据泄露控制技术机制，包括但不限于数据分布式处理过程中的调试信息、日志记录、缓存数据、中间数据等安全保护技术机制；

f) 应制定数据分布式计算节点的服务组件自动维护策略和管控措施，宜建立虚假节点监测、故障节点自动修复等技术机制，避免云计算环境或虚拟计算环境下潜在的对数据处理算法、机器学习模型的网络攻击。

6.4.2 大数据分析

要求包括：

a) 应建立大数据分析相关数据源的数据获取、汇聚及使用操作规范，明确大数据分析相关数据获取、汇聚及使用方式、访问接口、授权机制等；

b) 应在进行大数据分析前，对多数据源的汇聚数据开展安全风险评估，建立多源数据聚合、关联分析等数据资源操作规范和安全控制实施规范；

c) 应建立大数据分析结果的安全风险评估流程，控制基于大数据分析结果的数据使用、数据提供、数据公开等数据处理活动；

d) 应在遵循公平公正、公开透明、科学合理和诚实信用等原则的前提下，开展算法推荐服务或基于自动化决策服务，并向用户提供自动推荐功能关闭及参数配置等功能；宜建立多方参与的算法推荐服务安全管理制度和算法治理机制，具备对第三方提供集成算法的审核能力；

e) 应定期审计大数据分析过程记录和分析结果的存储、使用、提供等数据处理活动的合规性，具备对大数据分析结果和分析算法执行真实性进行溯源的能力；

f) 宜具备构建大数据分析过程及数据血缘图谱的能力，根据血缘关系对大数据分析数据及其衍生数据实施一致的管控。

6.4.3 密文计算

要求包括：

a) 宜具备对密文数据进行搜索、排序、计算等数据操作透明处理的能力；

b) 宜具备验证密文计算数据真实性、正确性的能力；

c) 应明确需要进行密文计算的数据资产和密钥管理技术机制，可自动或人工选择相适应的密码协议和机制，对密文计算过程进行保护；

d) 应具备保存密钥使用和密文计算日志存证的能力，支撑密文计算行为可追溯。

6.4.4 数据脱敏

要求包括：

a) 应建立数据脱敏管理操作规范，明确数据脱敏规则、脱敏方法和使用限制，包括脱敏后数据的可恢复性评估机制；

b) 应明确梳理出需要脱敏的数据资产，制定不同类别、级别数据的脱敏处理流程；

c) 应配置数据脱敏的技术工具或服务组件，支持如泛化、抑制、干扰等数据脱敏技术；宜具备对非结构化数据进行脱敏处理的能力，以及对脱敏处理效果的验证能力；

d) 应支持在数据脱敏时保留其原始数据格式和特定属性，以满足基于脱敏数据的开发与利用服务要求；

e） 应对数据脱敏处理过程相应的操作进行记录，以满足数据脱敏处理安全审计要求。

6.5 数据传输

要求包括：

a） 应区分安全域内、安全域间的数据传输场景，建立安全域内、安全域间不同场景的数据传输安全策略，通过部署安全通道、数据加密等措施保证大数据系统中数据传输的保密性和完整性；

b） 应建立大数据系统中数据传输接口安全管理操作规范，包括建立跨安全域的数据安全传输相关的符合国家密码管理规定的密钥管理和加密操作接口规范；

c） 应具备在构建传输通道前对两端主体身份进行标识和鉴别的能力，以及在跨域传输数据前对传输双方的数据安全级别进行评估的能力，避免将高安全等级数据传输到低安全等级的安全域；

d） 应具备对传输数据的完整性进行验证的能力以及相应的恢复控制措施；

e） 应具备对数据传输安全策略的变更进行审核和监控的能力，包括对通道安全配置、密码算法配置、密钥管理等保护措施的审核及监控的能力；

f） 应建立数据传输链路的冗余、恢复机制，保证数据传输链路的可靠性，并采用断点续传、超时重新连接等技术机制保障数据传输任务的可靠性。

6.6 数据提供

6.6.1 组织内提供

要求包括：

a） 应建立组织内跨安全域数据提供安全操作规范，明确数据提供活动涉及的职能部门和岗位相关的用户职责和权限，保证组织内数据提供安全策略的有效性；

b） 应审核组织内跨安全域提供数据的应用场景及其数据内容，检查数据接收方的数据使用和数据加工未超出其授权范围；

c） 应对数据提供活动进行监控，并采用数据加密、安全通道等管控措施提供数据，定期评估数据提供通道的安全性；宜利用专业的数据提供工具或组件对数据提供活动进行自动化安全保障；

d） 应制定数据提供活动安全审计策略和审计日志管理操作规范，记录数据提供活动日志，为数据提供相关安全事件的处置、应急响应和事后调查提供证据支撑；

e） 应在数据提供活动完成后对数据提供通道的缓存数据及相关临时数据进行安全删除。

6.6.2 跨组织提供

要求包括：

a） 应建立跨组织数据提供的数据风险评估操作规程，涉及数据共享、转让或委托处理时应与数据接收方通过合同、协议等形式明确双方的数据安全保护责任和义务；

b） 依法向其他组织提供其处理的个人信息时，应向个人信息主体告知数据接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并分别征得个人信息主体的单独同意；

c） 应建立跨组织数据提供的安全事件处置机制，发生重大事件时，及时终止数据提供，并要求数据接收方按 6.8 的要求销毁已接收的数据；

d） 在向境外组织提供重要数据和敏感个人信息前，应组织开展数据出境安全自评估，并通过法律法规要求的数据出境安全评估；

e） 应督促和监督数据接收方加强数据安全管理，发现其未落实合同规定要求和责任时督促数据

接收方及时整改，必要时终止数据提供活动，并监督数据接收方按6.8的要求销毁已接收的数据；

f) 应通过合同、协议等形式与数据接收方建立责任管理机制，对接入的数据接收方发生兼并、重组、破产时，要求数据接收方继续履行相关数据安全保护义务；对于没有能力继续履行相关义务的，要求数据接收方以合同中约定的形式返还、销毁其接收和产生的数据，签订数据销毁确认书；

g) 应具备对嵌入的第三方数据提供自动化工具进行安全监测的能力，当发现数据处理活动超出双方约定的合同或协议时及时停止第三方自动化工具的数据接入服务；

h) 应建立必要的数据出境管控技术机制，如要求数据接收方提供数据安全保护能力的证明，保证数据脱敏处理不可逆等；

i) 应在委托处理、向其他组织提供、公开或向境外提供个人信息时，进行个人信息保护影响评估，并对处理情况进行记录，个人信息保护影响评估报告和处理情况记录至少保存3年，共享、交易、委托处理重要数据的审批记录、日志记录至少保存5年；

j) 应在必要时对数据接收方的数据销毁机制进行验证，检查跨组织数据提供服务到期后其在数据接收方无数据残留，并签订数据销毁确认书。

6.7 数据公开

6.7.1 数据发布

要求包括：

a) 应建立数据主动公开发布管理制度和操作规范，明确发布数据使用者的权利和义务；

b) 应建立数据发布的管理措施与机制，包括数据发布的方式、范围，以及数据内容审核及审批制度；

c) 应提供数据发布清单，包括发布数据摘要、数据格式、更新频率等内容，以及使用条件等；

d) 应提供发布数据的数据访问接口及数据格式规范，宜具备对敏感个人信息等自动识别和实时脱敏处理等能力，保证大数据使用者能高效地获取发布数据；

e) 应具备对待发布数据进行重要数据及敏感个人信息识别能力，根据发布范围，发布对象等维度评估数据发布带来的数据安全风险，控制涉及重要数据、敏感个人信息等的数据的公开发布，经法律授权或具备合理事由确需公开披露的遵循相关规定进行；

f) 应定期审核发布数据资源的使用报告，在涉及用户数量巨大、数据处理活动对社会影响大时发布社会责任报告，包括数据保护措施、发生的安全事件及应对处理情况等内容。

6.7.2 在线访问

要求包括：

a) 应建立组织外用户在线访问准入准则和公开数据在线访问的授权操作规范与数据使用操作规范，包括访问申请的登记、审核、审批、办理、归档等工作制度，明确在线访问申请管理的审核内容；

b) 应建立组织外用户在线访问公开数据的数据使用责任追究技术机制，包括在线访问中安全事件应急保障处理流程及管控措施；

c) 应建立公开数据在线访问目录库和组织外用户在线访问公开数据的渠道，包括数据访问接口及格式规范，如提供机器可读的可扩展标记语言格式，使用户能高效地访问公开数据资源；

d) 应通过大数据平台服务组件实现组织外用户在线访问公开数据的申请的登记、审核、审批等管

理功能，提供包括用户身份鉴别、访问服务等服务组件的互认等安全管控功能；

e) 应采用自动和人工审计相结合的手段对在线访问操作进行监控和记录；涉及对重要数据等高风险数据操作的未经授权访问操作宜具备自动化识别和实时预警能力。

6.8 数据销毁

6.8.1 数据删除

要求包括：

a) 应建立数据删除安全操作规范，建立法律法规要求的重要数据或个人信息多级级联删除操作模式，明确大数据服务停止运营、用户账户注销、用户申请数据删除等场景的数据安全删除的操作规程；

b) 应建立物理删除和逻辑删除的数据删除方法和技术，明确不同类别和级别的数据删除方式和技术要求；

c) 应建立不可逆数据删除机制，配置必要的数据删除工具，能根据业务场景需求以不可逆方式删除相关的数据及其衍生的各种副本数据；

d) 应在行政机构、司法裁定等指定删除数据时，或达到存储期限，或用户主动提出数据删除请求，注销账户或者变更、撤销授权时，以及因使用自动化采集技术等无法避免收集到的非必要个人信息时，在约定时间进行数据删除或进行匿名化处理，使个人信息及相关数据不可访问或不可重新标识；

e) 应建立动态的数据删除机制，主动、及时删除已实现数据处理目的或者实现处理目的不再必要的数据，包括数据处理过程中备份数据、衍生数据及操作日志数据等；

f) 应建立数据删除效果评估和复核机制，定期检查已被删除的数据是否还能访问；

g) 应监督数据删除操作及其删除效果反馈的过程，包括已共享或者已被其他用户使用的数据的删除技术管控措施，跟踪和记录数据删除活动，具备对数据删除操作的追溯能力。

6.8.2 介质管理

要求包括：

a) 应建立大数据系统存储介质访问和使用管理规范，对存储介质进行标记，明确存储介质的数据类型，采取有效的介质净化技术和操作规程对存储介质进行净化；

b) 应依据介质存储数据类型和重要性明确磁介质、光介质和半导体介质销毁方法和机制；

c) 应按照法律法规和标准规范销毁存储介质，使用经认证的物理销毁设备或请具备资质的单位对存储重要数据和个人信息的介质设备进行物理销毁；

d) 应制定存储介质销毁的监管措施，对销毁介质登记、审批、交接等介质销毁过程进行监控；

e) 应建立介质管理系统，对存储介质的使用和传递过程进行全程跟踪，对介质访问、使用、销毁等过程进行记录和审计，并定期对销毁记录及介质销毁效果进行检查。

7 大数据服务安全风险管理能力

7.1 风险识别

7.1.1 数据安全风险识别

要求包括：

a) 应采用接口扫描、流量分析、业务监测等方式构建数据资产识别能力，及时对数据处理活动相关的数据源信息、数据资产等进行标识，并更新数据资产目录；
b) 应对数据处理活动组件进行威胁及脆弱性识别，分析其对大数据服务的安全影响，形成数据安全风险分析报告，必要时将风险应对的建议措施报送给数据安全管理机构审批；
c) 应具备基于数据安全风险分级和按照国家数据分类分级相关制度对数据资产进行分类分级的能力，宜通过技术手段对识别到的数据资产类别、级别等安全属性进行自动化标记；
d) 应针对应用于关键信息基础设施的大数据平台提供定制化的数据处理和大数据系统运营的安全控制措施，且通过主管部门认可的第三方评估机构的评估；
e) 应建立数据处理活动安全风险知识库，对大数据系统运营日志进行汇聚和融合分析，宜自动生成大数据服务涉及的数据安全风险信息；
f) 应针对数据提供、数据使用、数据加工等数据处理活动，或钓鱼邮件、勒索病毒等安全风险场景，定期进行数据业务或数据对象安全管控措施的隐患排查和治理，提升数据安全风险识别能力和应对能力；
g) 应定期自行开展或邀请第三方专业机构开展数据安全风险识别和风险分析工作，按规定保存数据安全风险分析报告，包括识别风险应对情况记录等信息。

7.1.2 供应链安全风险识别

要求包括：

a) 应定义大数据服务中数据供应链上下游组织的数据交换共享的格式规范、接口规范，约定数据提供和数据获取方式等技术或管理措施，使大数据系统中上下游组织的数据流通管控操作透明和可识别；
b) 应具备发现大数据服务中数据供应链上下游组织网络产品和服务的脆弱性和威胁的能力，包括根据适用法规和合同要求进行综合分析并形成数据供应链风险分析报告的能力，必要时将风险应对的措施报送给数据安全管理机构审批；
c) 应向大数据服务中数据供应链上下游的组织及时发布所识别的数据供应链风险及风险应对建议，保证数据供应链中数据收集、数据提供和数据公开等数据处理活动的数据安全风险可控；
d) 应基于主管部门的监管要求，定期对数据供应链上下游组织的数据处理活动中的数据安全风险、支撑大数据服务的网络产品和服务的安全技术和措施有效性进行分析评估，按规定保存数据供应链安全风险分析报告，包括识别风险、应对情况记录等信息。

7.2 安全防护

7.2.1 区域边界防护

要求包括：

a) 应对大数据服务涉及的区域边界进行划分，并采取区域边界防护措施，制定区域边界数据流转操作的安全策略和操作规程；
b) 应对跨区域边界的数据使用、提供、公开等数据处理活动防护措施进行检查，保证数据安全责任不随数据跨区域边界转移而改变，在不同区域间的数据安全策略实施效果保持一致；
c) 应制定区域边界防护策略和规程的更新维护规则，并采用必要的手段或管控措施使更新后区域边界防护策略与规程得到实施；
d) 应在涉及重要数据和个人信息的跨组织的区域边界访问时，对应用接口或服务接口等访问进行主客体的双向身份鉴别，保证不同区域边界之间的安全管控措施有效并与风险程度相适应；

e) 应建立基于主客体属性和区域边界上下文的逻辑访问控制措施及机制，实现跨区域边界的大数据使用者动态授权与数据访问控制。

7.2.2 计算环境防护

要求包括：

a) 应建立数据感知、保护、预测、响应等一体化的多层次安全防护体系，满足网络安全等级保护等制度的纵深防御要求；
b) 应根据数据安全风险管理制定安全基线配置清单，启用、禁止或限制大数据平台和大数据应用特定的功能、端口、协议或服务；
c) 应建立终端智能设备、第三方或开源系统与服务组件等计算设施接入约束规范；宜采用技术工具对大数据服务的接入设备、服务组件及数据处理系统等计算设施的安全属性进行管理；
d) 应制定计算环境安全初始化策略，包括数据存储等大数据服务模块自启动检查机制，保证计算环境在故障重启后的数据完整性和一致性；
e) 应制定满足可靠性与可用性的计算环境垂直扩展、水平扩展策略，提供海量数据或复杂类型数据高效处理方法及其安全保护技术与机制；
f) 应建立统一身份管理技术平台，支持用户账户、授权、认证、审计等安全数据统一管理；涉及处理重要数据和个人信息用户身份鉴别与授权管理宜提供独立的物理服务器；
g) 应提供细粒度授权管理和访问控制功能，如依据资产属性和用户属性设置授权规则和访问控制措施等，以支持分布式计算环境中大数据分析及人工智能算法迁移的安全性；
h) 应具备分布式用户身份鉴别、访问控制，安全审计等安全数据的关联巡检功能，能对大数据服务元数据完整性进行核查，提供禁用非法账号、闲置账号、过期账号及彼此间的关联关系分析和管理能力。

7.2.3 数据操作防护

要求包括：

a) 应制定数据供应链中数据流转操作安全管控策略，通过技术机制对大数据系统以及供应链涉及的数据流转操作进行控制；
b) 应响应数据主体对于个人信息或数据查询、复制、更正、补充，以及转移至指定数据接收方的请求，在符合数据主体要求条件时，提供个人信息转移的安全途径；
c) 应建立高风险数据操作清单及其管控措施，如在人工进行高风险数据操作时采用双人、双账户鉴别后协作完成，以及在程序自动进行高风险数据操作时宜通过基于密码技术鉴别的数据服务接口进行实现等；
d) 应部署数据防泄露、数据脱敏、个人信息去标识化等安全功能组件，具备防范使用网络爬虫技术、数据分析技术等从网络层和应用层获得重要数据和个人信息的能力；
e) 应在大数据服务相关数据操作系统或组件下线，以及相关智能终端设备退网时，执行规范的数据转移、转存或删除操作，防止数据泄露；
f) 因业务确需向境外提供个人信息或重要数据时，应在通过国家主管部门组织的数据出境安全风险评估的基础上，要求境外数据接收方提供适当的数据安全保护能力证明。

7.2.4 数据服务接口防护

要求包括：

a) 应制定数据服务接口安全控制策略，明确规定使用接口的安全限制条件和安全控制措施，如身份鉴别、授权策略、访问控制、数字签名、时间戳、安全协议、白名单制等；
b) 应建立数据服务接口清单，明确数据服务接口安全规范，包括接口名称、接口参数、接口安全要求等，具备对接口不安全的输入参数进行限制或过滤的能力，并提供异常处理功能；
c) 应具备对重要数据、个人信息等重要数据操作服务接口的调用进行记录、汇聚和集中存储的能力，并具备通过大数据分析技术进行数据服务接口的风险识别和安全性分析的能力。

7.2.5 威胁信息分析

要求包括：

a) 应具备对数据处理活动相关的威胁情报数据的收集、存储、管理和利用能力，掌握大数据服务涉及数据处理活动所面临的威胁信息；
b) 应具备对数据资产攻击、系统脆弱性利用等安全事件监测能力，对引起大数据服务安全态势发生变化的安全属性进行获取，对大数据服务的安全态势进行多维度展示；
c) 应具备对威胁情报数据的关联分析能力，以及将威胁情报数据向大数据服务安全检测防御规则或控制措施的转化能力；
d) 应与专业机构建立威胁情报数据共享机制，持续提高数据安全风险和供应链安全风险应对处置和防范能力；
e) 宜采用自动化技术机制，对多源异构威胁情报数据进行归并、融合和分析，对安全事件的发展趋势进行预测，并进行主动、协同式的数据安全威胁检测和应急处置。

7.3 安全监测

7.3.1 数据处理监测

要求包括：

a) 应建立数据处理活动及其数据操作服务接口的安全监测措施，宜具备对数据处理活动及其数据操作服务接口的访问进行自动化监控和应急处置的能力；
b) 应建立数据处理活动的监测规则，能根据预定义的数据安全基线或阈值对数据处理活动异常行为进行告警，并展示数据处理活动发生的位置、操作以及数据处理活动的风险及威胁等信息；
c) 应具备对数据处理过程和存储数据使用与访问进行监测的能力，及时发现违规数据处理行为，记录并安全存储监控日志 6 个月以上，以满足数据处理活动安全审计要求；
d) 应建立针对重要数据和敏感个人信息流转等敏感数据操作的监测机制，并采取技术措施及时发现对这些数据的违规操作或数据泄露等安全风险；
e) 应部署数据防泄漏监控工具，对异常或高风险的跨区域边界的交换、共享等数据提供行为进行实时监控，发现异常时自动阻断数据传输。

7.3.2 系统运行监测

要求包括：

a) 应建立大数据系统运行监测平台，支持分布式计算节点的处理器、内存、磁盘、网络流量等计算资源状态及其支持大数据服务状态的统一监测；
b) 应对分布式计算节点的用户身份鉴别和数据访问情况进行采集、存储和安全性分析，具备对计算节点接入、用户授权访问及数据使用等安全风险的监测和分析能力；

c) 应具备对大数据系统越权访问、高频访问、恶意操作等运行异常行为的发现、记录、统计和分析能力，并按重要程度和影响程度对大数据系统运行异常行为进行分级告警；
d) 应具备对数据供应链、数据委托处理、第三方服务组件等重要业务相关应用和涉及重要数据和个人信息处理过程相关应用的监测能力，对系统运行状况及其数据流转操作情况等进行监测；
e) 应建立大数据系统存储设施的健康监测、多副本冗余、纠删码冗余、数据自动修复等机制，保证大数据系统及所控制数据的完整性和可用性；
f) 应制定系统运行监测安全审计策略，记录并安全存储系统运行日志 6 个月以上，为系统安全检查、安全响应、安全恢复等相关事件处置、应急响应和事后调查提供证据支撑。

7.3.3 服务持续监测

要求包括：

a) 应依据 5.1 策略与规程的要求，制定大数据服务持续监控机制，明确数据服务接口、业务连续性、供应链安全等服务水平协议监测指标和频率，对大数据服务安全措施进行持续监测；
b) 应跟踪和控制大数据服务相关的网络产品和服务及其数据访问接口，及时终止不安全的网络产品和服务组件运行，记录并安全存储监控日志 6 个月以上，以满足大数据服务安全审计要求；
c) 应对监测累积的大数据服务监测记录进行关联和分析，必要时向数据安全管理机构报送大数据服务及其数据资产的安全风险信息；
d) 应使用监控工具维护大数据服务监控信息的准确性、真实性，持续落实针对数据安全风险和供应链安全风险的应对措施等。

7.4 安全检查

要求包括：

a) 应定期对大数据系统的安全控制措施进行检查，使所采取的安全措施覆盖了不同级别的数据安全防护要求，并与大数据系统安全运营风险程度相匹配；
b) 应按照上级主管部门要求、专业安全机构建议，定期安排或在爆发网络攻击、重大安全漏洞时，及时开展专项安全检查；
c) 应跟踪数据安全和个人信息保护相关法律法规和管理规定，结合大数据系统运营中的数据安全风险情况，及时制定、完善组织内部的数据处理安全检查评估内容，定期开展通用和专项数据安全和供应链安全检查评估工作；
d) 应在法律法规修订、组织业务重组、组织业务模式或运行环境发生重大变更、或发生重大的数据安全事件时，及时地对数据保护措施进行安全影响评估；
e) 应在获得授权同意以及做好风险管理和应急预案等工作前提下，采取渗透性测试方式对数据处理活动及其组件进行安全风险评估；涉及重要数据的大数据系统，应获得相关主管部门批准后方可实施漏洞探测、渗透性测试等安全检查评估活动。

7.5 安全响应

7.5.1 应急预案管理

要求包括：

a) 应建立大数据服务应急预案，包括应急组织机构与职责、安全事件分类分级、监测与预警、应急处置流程、保障措施等内容，且应急预案经本单位审核通过后，按要求报主管部门备案；

b) 应开展大数据服务应急预案培训，培训内容覆盖全流程的数据处理活动、关键业务及数据安全应急所需的安全应对控制措施；
c) 应建立大数据服务应急预案演练计划，定期开展应急演练，保存演练记录和演练总结报告，在大数据系统本身、外界环境发生重大变化时，对应急预案进行更新，保留审核发布记录；
d) 应与主管部门、第三方安全机构及其他相关职能部门间，建立大数据服务应急处理、协调、沟通渠道；
e) 应建立大数据服务安全应急响应知识库，包括数据泄露、数据篡改、数据破坏、网络勒索等不同类型的安全事件及处置办法，并用于应急响应培训及演练计划。

7.5.2 安全事件处置

要求包括：

a) 应建立安全事件处置操作规程，明确安全事件的处置方法，包括不同安全事件分类分级、启动条件及所需的资源，不同类别、级别事件的响应、处置和报告流程；
b) 应明确大数据系统遭受破坏时，恢复关键数据业务和全部数据业务的预期处理时间，并在大数据系统发生故障、受到损害或发生中断时，在指定的时间内完成关键业务的恢复；
c) 应及时向主管部门、可能受影响的组织和人员通报安全事件；
d) 应在发生有可能危害重要数据或危害国家安全等关键业务的安全事件时，立即组织研判，在规定时间内形成安全事件报告，按规定及时向数据安全管理机构上报；
e) 应在安全事件涉及个人信息时，及时告知受影响个人信息主体，涉及一定数量规模的个人信息的，按规定及时向数据安全管理机构上报；
f) 应在安全事件处置完成后，及时调查安全事件的直接原因和间接原因、经过、责任，评估安全事件造成的影响和损失，总结安全事件防范和应急处置工作的经验教训，提出处理意见和改进措施，形成安全事件处置报告。

7.5.3 事件归因分析

要求包括：

a) 应制定安全事件归因分析的数据溯源策略和安全管理机制，以及事件归因溯源数据安全存储与使用的管理制度；
b) 应跟踪和记录数据处理活动及其相关的数据服务，支持数据处理活动事件可溯源，包括对日志记录的使用、提供和公开等数据处理活动进行细粒度安全审计；
c) 宜支持根据时间顺序、攻击来源、攻击对象等对数据处理活动和大数据服务中的攻击行为进行关联分析，提高数据安全事件溯源分析能力；
d) 应采用数字水印、数据标记、可信存证等技术保障数据处理过程的可追溯性；
e) 应对事件归因的溯源数据进行备份或归档，并采取技术手段对重要数据和个人信息处理活动的溯源数据进行安全保护；
f) 应采取技术机制和管控措施保证事件归因的溯源数据完整性，通过溯源数据能重现数据处理活动的全过程；
g) 宜建立基于溯源数据的数据业务合规性审核机制，并依据审核结果改进大数据服务相关的访问控制、合规性保障等数据安全策略及其安全技术机制。

7.5.4 安全风险报送

要求包括：

a) 应建立重要数据和个人信息异常处理上报机制，当重要数据或个人信息发生泄露、非法篡改等情况时，及时采取处置措施，并按规定及时告知用户，形成安全事件报告报送相关主管部门；
b) 应对涉及重要数据和个人信息的数据处理活动及其数据供应链活动，按规定定期开展安全风险评估，并向有关主管部门报送安全风险信息，风险评估报告包括处理的重要数据和个人信息的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等；
c) 应针对安全监测、安全检查等风险管理中发现的安全隐患，立即采取措施，将安全事件处置等形成的安全风险信息，经数据安全管理机构审批后依据国家相关规定向主管部门上报；
d) 应在经过数据出境评估后向境外组织提供重要数据和数据出境达到相关规定数量的个人信息时，形成安全风险信息，经数据安全管理机构审批后依据国家相关规定向主管部门上报。

7.6 安全恢复

7.6.1 数据恢复

要求包括：

a) 应识别需要备份和归档的数据，制定数据备份、归档与恢复的计划；
b) 应配置必要的数据备份、归档与恢复工具，采用技术手段记录数据备份、归档与恢复过程，支持数据备份、归档与恢复过程可溯源；
c) 应定期测试数据备份、归档和恢复安全管控措施，对备份和归档数据的可用性、完整性和一致性进行检测，对数据恢复的安全风险进行分析，具备基于备份和归档数据的数据恢复能力；
d) 应结合业务需求和安全目标，定期或按需开展数据恢复实战演练。

7.6.2 业务恢复

要求包括：

a) 应建立大数据系统的容灾备份和灾难恢复管理制度，明确系统在建设规划、运行维护、应急响应和灾难恢复中需要满足的业务连续性的安全运行要求；
b) 应制定大数据系统灾难恢复预案，明确大数据系统灾难恢复的范围和目标、灾难切换规程和操作手册、灾后重建运行操作指南，定期组织灾难恢复预案的培训和演练；
c) 应建立灾难恢复运行监控平台，具备容灾备份系统的有效性验证能力，及时发现容灾备份系统的运行故障；
d) 应定期开展大数据系统灾难恢复演练，根据演练情况修订灾难恢复预案等业务连续性计划，检查系统容灾备份和灾难恢复预案的有效性；
e) 应建立异地容灾备份和恢复操作规范，配置系统容灾备份和灾难恢复专业团队，具备按照业务系统重要性和受影响程度及时接管大数据系统的数据处理活动的能力。

参 考 文 献

[1] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系要求

[2] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南

[3] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

[4] GB/T 24353—2009 风险管理 原则与实施指南

[5] GB/T 31168—2023 信息安全技术 云计算服务安全能力要求

[6] GB/T 35589—2017 信息技术 大数据 技术参考模型

[7] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

[8] ISO/IEC 27002 Information security, cybersecurity and privacy protection—Information security controls

[9] NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations