ICS 35.020
CCS L 80

DB21

辽　宁　省　地　方　标　准

DB21/TXXXX—XXXX

工业数据流通　数据分级保护要求

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

辽宁省市场监督管理局　发布

目　次

前　言

本文件按照GB/T1.1-2020《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。

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。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：沈阳华睿博信息技术有限公司等。

本文件主要起草人：邵华等。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

归口管理部门通信地址：辽宁省沈阳市皇姑区北陵大街45-2号。

归口管理部门联系电话：024-86913384。

标准起草单位通讯地址：辽宁省沈阳市和平区青年大街386号华阳国际大厦2396。

标准起草单位联系电话：18698849086。

工业数据流通 数据分级保护要求

1 范围

本文件规定了工业数据流通过程中数据分级、采集、存储、使用、加工、传输、共享、开放、销毁、出境、转移以及委托处理等方面的要求。

本文件适用于指导工业数据流通过程中工业数据的分级安全保护。

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 5271.1—2000 信息技术 词汇 第1部分：基本术语

GB/T 41778—2022 信息技术 工业大数据 术语

DB21/T 3867-2023 工业数据分类分级管理指南

3 术语和定义

以下术语和定义适用于本文件。

3.1

数据 data

信息的可再解释的形式化表示，以适用于通信、解释或处理。

[来源：GB/T 5271.1—2000,01.01.02]

3.2

工业数据 industrial data

工业领域产生和收集的数据，包括研发设计、生产制造、经营管理、运行维护、平台运营等过程中收集和产生的任何以电子或者其他方式记录的数据。

3.3

工业数据采集 industrial data collection

利用采集装置,对工业设备、信息化系统、自动化系统和环境等工业系统产生的数据进行收集的过程。

[来源：GB/T 41778—2022,3.23]

3.4

工业数据存储 industrial data storage

工业数据以某种格式记录在计算机内部或外部存储介质上的行为。

3.5

工业数据使用 industrial data use

使用工业数据来完成某项现实任务。

3.6

工业数据加工 industrial data processing

通过对工业数据进行数据挖掘、分析、加工等活动，获取目的结果的行为。

3.7

工业数据传输 industrial data transmission

工业数据从一个系统、设备、平台、企业传送到另一个系统、设备、平台、企业的通信过程。

3.8

工业数据共享 industrial data openness

工业数据处理者向其他数据处理者提供数据,或将工业数据处理权由一个处理者向另个处理者转移，且双方分别对数据拥有独立处理权的过程。

3.9

工业数据开放 industrial data openness

指将工业数据免费开放给每一个希望使用数据的人，没有版权、专利和控制机制等的限制。

4 工业数据分级

应按照DB21/T 3867-2023中的要求对工业数据进行分级。

5 工业数据采集

5.1 一般数据

一般数据采集的安全防护要求如下：

a） 工业数据采集应符合“合法、正当、必要”原则；

b） 工业数据采集设备应符合安全认证，采集流程和方式应符合相应要求；

c） 采取必要的措施保障个人数据和重要数据的安全，工业数据采集过程中，对数据主体合法权益造成的损害承担责任；

d） 只采集满足数据主体授权同意的目的所需的最少数据类型和数量；

e） 以明确、易懂和合理的方式公开采集数据的范围、目的、规则等，并接受外部监督；

f） 工业数据采集过程中，应加强对数据源鉴别；

g） 设立负责数据源鉴别和记录的岗位和人员，对采集的数据源进行鉴别和记录；

h） 制定数据源管理的制度规范，定义数据溯源安全策略和溯源数据格式等规范，明确提出对数据源进行鉴别和记录的要求；

i） 采取技术手段对外部收集的数据和数据源进行识别和记录；

j） 对关键溯源数据进行备份，并采取技术手段对溯源数据进行安全保护；

k） 通过身份鉴别、数据源认证等安全机制确保数据来源的可靠性；

l） 工业数据采集过程中，应加强对数据的质量管理，数据的质量应从真实性、完整性、规范性、一致性、准确性、唯一性、关联性、时效性等维度进行衡量；

m） 工业数据采集时应标记数据的类别级别。

5.2 重要数据

重要数据采集在 4.1 的基础上还应满足以下要求：

a） 根据工业数据采集需求，应明确采集目的、方式、数量、用途、获取源、接收方、范围、频率和周期等，确立工业数据采集规则，保障采集的数据的安全可用；

b） 在工业数据采集前，应对工业数据采集所涉及的软硬件工具、设备、系统、平台、接口以及采集技术等，采取必要的测试、认证、鉴权等措施，保证工业数据采集的合规性和执行上的一致性；

c） 应对工业数据采集的时间、范围、类型、数量、频度、流向、级别等信息进行记录和审计，避免出现超范围工业数据采集活动；

n） 应采取加密方式对数据进行保护；

d） 应具备对工业数据采集行为进行监测的技术能力，并能够在发现异常时进行告警；

e） 通过间接途径获取数据的，应与数据提供方通过签署相关协议、数据源合法性书面承诺等方式，明确双方法律责任；

f） 在工业数据采集后，数据源及流转中间设备应删除相关数据，不应私自留存；

g） 应采取必要的防泄漏技术或手段，防止工业数据在采集过程中发生泄露；

h） 通过间接途径获取的数据，数据处理者应与数据提供方签署相关协议、承诺书等方式，明确双方法律责任。

5.3 核心数据

核心数据采集在 4.2 的基础上还应满足以下要求：

a） 应具备工业数据采集行为实时监控能力，在发现异常时第一时间终止工业数据采集行为；

b） 应使用水印溯源等技术，对数据泄露风险及行为进行追踪，可定位到责任人等。

6 工业数据存储

6.1 一般数据

一般数据存储安全防护要求如下：

a） 工业数据应保存在可信或可控的信息系统或物理环境中；

b） 应根据存储数据量、数据重要性、数据敏感程度等因素，选择合适的存储介质，实施工业数据存储介质安全管控；

c） 应加强对隐形敏感数据的识别，例如有些数据在法律法规中并未被认定为敏感数据域范围，这类数据单独使用时无任何敏感性可言，但结合其它数据，却可以组合成为敏感数据；

d） 应设立工业数据存储介质安全管理部门，对工业数据存储介质进行统一管理；

e） 工业数据存储介质采购应选择可靠的品牌，优先考虑国产品牌，确保产品质量，采购时遵循申报、审批、采购、标识、入账的流程，采购中应进行防病毒等安全性检测，在确保安全的情况下入账；

f） 工业数据存储介质的存放环境应有防火、防盗、防水、防尘、防震、防腐蚀及防静电等措施，防止其被盗、被毁、被未授权修改以及其信息的非法泄露；

g） 应对工业数据存储介质作明确的分类标识，包括存储数据的内容、归属、大小、存储期限、保密程度等，并结合数据类型和管理策略统一命名；

h） 应建立工业数据存储介质保管清单，由工业数据存储介质安全管理部门定期根据保管清单对介质的使用现状进行检查，检查内容包括完整性和可用性，出现差异时，必须及时报告给上级领导部门；

i） 工业数据存储介质在运输过程中，必须采取密封处理；

j） 当存有敏感业务信息的工业数据存储介质进行异地传输时，应选择本单位可靠人员进行传递，并且使用专用安全箱包进行包装；

k） 应选取可靠的速递公司承担工业数据存储介质的传递工作，应与速递公司签订协议，明确工业数据存储介质传递时间、安全保障（防火、防震、防潮、防磁、防盗）等方面的要求，速递公

司的资质、介质传递流程、速递合同须经存储介质安全管理部门批准；

l） 工业数据存储介质安全管理部门需对工业数据存储介质的运输过程进行详细记录；

m） 逻辑存储系统应对用户进行权限分离，授予用户最小的权限；

n） 逻辑存储系统账号口令要严格保密，并要求具有一定的复杂度（例如最小长度不小于 8 位,至少包含大写字母、小写字母、数字和特殊字符），账号口令需定期更改，账号口令的更新周期不得超过 90 天；

o） 应具备较强的病毒防范意识，定期进行病毒检测，发现病毒立即处理并通知上级领导部门或专职人员；

p） 定期检查逻辑存储系统上的安全日志进行检查，对错误、异常、警告等日志进行分析判断，并将判读结果进行有效解决处理并记录存档；

q） 应在获得客户的授权的前提下，工业企业才具有客户数据的管理权限；

r） 应依据法律规定或与用户约定的方式和期限存储数据，并根据实际情况开展数据备份。

6.2 重要数据

重要数据存储在 5.1 的基础上还应满足以下要求：

a） 应采用工业数据存储介质安全管控、校验技术、加密技术、数字签名等手段实现数据安全存储，不得直接提供存储系统的公共信息网络访问；

b） 应对存储数据的使用者进行身份鉴别和访问控制；

c） 应能够检测到数据在存储过程中机密性、完整性、可用性收到破坏，在检测到数据被破坏时进行告警并采取必要的恢复措施；

d） 应提供有效的虚拟机镜像文件加载保护机制，保证即使虚拟机镜像被窃取、非法用户也无法直接在其计算资源上进行挂卷运行；

e） 重要工业数据应存储于中国境内，如需出境，应遵循国家相关规定；

f） 应加强数据备份管理，并对备份的数据采取与原数据同等级别的安全措施；

g） 应定期进行数据恢复演练，全量数据备份至少每周一次，增量数据备份至少每天一次；

h） 应定期测试备份数据的完整性和可用性，以确保在需要恢复数据时可以顺利还原；

i） 应采取必要的防泄漏技术或手段，防止工业数据在存储过程中发生泄露。

6.3 核心数据

核心数据存储在 5.2 的基础上还应满足以下要求：

a） 应对核心工业数据存储设备进行硬件冗余，启用实时数据备份功能，并实施异地容灾备份，保证主设备出现故障时冗余设备可以实时切换并恢复数据；

b） 应具备工业数据存储行为实时监控能力，发现异常时第一时间终止数据访问、删除、修改等操作行为，并采用技术手段保证存储操作行为可溯源。

7 工业数据使用

7.1 一般数据

一般数据使用的安全防护要求如下：

a） 应建立工业数据使用过程中的相关责任和管控机制，严格按照国家相关法律法规和行业规范执行；

b） 工业数据使用者在使用数据前应明确工业数据使用目的，并向数据监管部门提交申请，申请内容至少包含申请人信息、所在部门、岗位、申请理由、申请内容等信息；

c） 数据监管部门在收到工业数据使用申请之后，需对所申请的工业数据使用范围及内容进行风险评估以及合规性审查等工作，工业数据使用监管部门审查无误后，方可对使用的数据的范围和内容进行授权，授权过程中应采取“最小够用”原则，即为工业数据使用者提供完成业务处理活动所需的最小数据集；

d） 当使用个人信息时，应征得个人信息主体的明示同意；

e） 数据监管部门有权对不合规的使用申请提出否决意见、对授权范围和内容的变更或终止提出意见；

f） 应对数据的访问权限和实际访问控制情况进行定期审计，至少每半年一次对访问权限规则和已授权清单进行复核，定期清理已失效的账号和授权。

7.2 重要数据

重要数据使用在 6.1 的基础上还应满足以下要求：

a） 应配置成熟的数据权限管理平台，限定用户可访问的数据范围；

b） 授权应当符合内部控制的基本要求，做到不相容岗位的有效分离；

c） 工业数据使用监管部门需确定授权的有效期，期满后需重新授权；

d） 应建立工业数据使用的违规处罚制度和惩罚措施，对个人信息，重要数据的违规使用等行为进行处罚，强调工业数据使用者安全责任；

e） 应采取必要的防泄漏技术或手段，防止工业数据在使用过程中发生泄露。

7.3 核心数据

核心数据使用在 6.2 的基础上还应满足以下要求：

a） 工业数据使用监管部门完成用户权限的设置后，必须将签署后的授权书存档备案管理；

b） 应配置成熟的工业数据使用日志记录或审计产品，对工业数据使用操作进行记录审计以备责任识别和追责；

c） 工业数据使用监管部门需监视数据的使用情况，发现可疑授权、可疑使用情况时，及时通报修正。

8 工业数据加工

8.1 一般数据

一般数据加工的安全防护要求如下：

a） 应对数据的访问权限和实际访问控制情况进行定期审计，至少每半年对访问权限规则和已授权清单进行一次复核，定期清理已失效的账号和授权；

b） 应建立数据导入导出过程保护和回退机制，在导入导出过程中发生问题时应能够有效还原和恢复数据；

c） 利用数据进行自动化决策的，应保证决策的透明度和结果公平合理；

d） 应对数据挖掘，关联分析等工业数据使用行为进行记录；

e） 应在不影响工业数据加工与分析的情况下，对数据脱敏后再进行处理；

f） 数据处理者提供数据处理服务，涉及经营电信业务的，应当按照相关法律、行政法规规定取得电信业务经营许可。

8.2 重要数据

重要数据加工在 7.1 的基础上还应满足以下要求：

a） 应对数据的加工行为进行访问控制，包括身份认证和授权等；

b） 应避免将挖掘算法产生的中间过程数据与原始工业数据存储于同一逻辑空间；

c） 应明确原始工业数据加工过程中的数据获取方式、访问接口、授权机制、逻辑安全、处理结果安全等内容，并周期性的检查用户操作数据的情况，统一管理工业数据使用权限；

d） 应采用恶意代码检测、身份鉴别、访问控制等技术手段保障处理数据的平台、系统、工具、APP 等安全；

e） 应对数据的加工进行记录和审计，并形成审计日志，日志至少包含明确的主体，客体、操作时

间、具体操作类型、操作结果等；

f） 应对原始数据和挖掘结果进行标识防止数据被恶意删除、篡改、滥用；

g） 应在不影响工业数据加工的情况下，对数据脱敏后再进行处理；

f） 应采取必要的防泄漏技术或手段，防止工业数据在加工过程中发生泄露。

8.3 核心数据

核心数据加工在 7.2 的基础上还应满足以下要求：

a） 应在不影响工业数据加工与分析的情况下，对需要用到的知识机理、数字化模型、算法、工具等进行测验分析，保证工业数据加工结果的准确性和安全性；

b） 应具备工业数据加工行为实时监控能力，在发现异常时第一时间总终止工业数据使用加工行为，并采用技术手段保证所有数据挖掘、使用、加工、分析等行为可溯源。

9 工业数据传输

9.1 一般数据

一般数据传输安全防护要求如下：

a） 应采用数据加密、数据脱敏、校验技术、安全传输通道或者安全传输协议等措施保证工业数据传输安全；

b） 实时控制系统工业数据传输，应使用独立的网络设备组网，在物理层面上实现与其他数据网络及外部公共信息网络的安全隔离；

c） 对于工业互联网平台数据，应保证平台客户可以根据业务需求自主选择边界数据的交换方式。

9.2 重要数据

重要数据传输在 8.1 的基础上还应满足以下要求：

a） 应采用数字签名等技术，保证工业数据传输过程中的机密性、完整性、可用性；

b） 应能够检测到数据在传输过程中机密性、完整性、可用性受到破坏，并在检测到数据被破坏时，采取必要的恢复措施；

c） 应采用 TLS/TLCP 等安全协议进行工业数据传输；

d） 应在数据迁移前对数据开展本地备份及恢复相关工作，做好数据迁移安全评估与安全控制，防止迁移过程中因突发状况导致数据丢失，避免影响业务应用的连续性；

e） 应在数据迁移、上云、跨境等传输过程中，开展数据安全监测，能够对网络流量行为、攻击威胁、数据泄露或篡改等进行分析和研判；

f） 应使用校验或密码技术保证工业互联网平台等数据载体间数据迁移过程的完整性；

g） 应具备工业数据传输异常检测技术能力，对陌生 IP 地址、数据库异常连接等进行实时告警，在检测到数据遭破坏时及时采取恢复措施；

h） 涉及跨组织机构或者使用公共信息网络进行工业数据传输的，应建立内部登记、审批机制；

g） 应采取必要的防泄漏技术或手段，防止工业数据在传输过程中发生泄露。

9.3 核心数据

核心数据传输在 8.2 的基础上还应满足以下要求：

a） 应具备工业数据传输实时监测处置能力，保证能够第一时间告警并阻断违规传输；

b） 应具备数据溯源能力，保证所有工业数据传输路径可恢复，工业数据传输行为可溯源；

c） 应采用密码技术手段实现工业数据传输的真实性、不可抵赖性和可控性。

10 工业数据共享

10.1 一般数据

一般数据共享安全防护要求如下：

a） 应对工业数据按照数据共享属性进行分类；

b） 对于分类属性为不共享的数据，不得共享；

c） 对于分类属性为受限共享、无条件共享的数据应满足以下要求：

1） 应明确数据共享的安全规范，从国家安全、组织机构的核心价值保护、个人信息保护等方面对数据共享的风险控制提出要求，明确相应的权限审批和授权流程，并根据不同场景下数据共享制定细化的规范要求；

2） 需建立工业数据共享的审核流程，包括共享的数据内容、涉及的部门和组织、授权审批同意/否决、归档记录等。尤其对于向外部提供的共享数据，一定要有严格的审核流程；

3） 组织需在工业数据共享的各个阶段加入安全审计机制，严格、详细地记录并保存工业数据共享的所有操作和行为，为工业数据共享安全事件的处置、应急响应和事后调查提供帮助。同时，工业数据共享安全管理部门需设置专人定期对工业数据共享相关的日志记录进行安全审计，发布审计报告，并跟进审计中发现的异常；

4） 应在工业数据共享前对工业数据共享的必要性、范围、规模、方式等进行分析研判，研判结果为可以共享的，应根据需要采取合适方法对数据进行脱敏处理，保证工业数据共享安全；

5） 需基于工业数据共享的场景，对所申请的共享的数据进行风险评估。如基于内部业务系统之间的共享或基于业务需要的对外共享等，根据工业数据共享涉及的数据范围、数据类型、数据内容及数据格式等评估不同场景的工业数据共享风险。

10.2 重要数据

重要数据共享在 9.1 的基础上还应满足以下要求：

a） 应根据实际情况，采取数据水印等必要措施保证工业数据共享安全；

b） 应采取密码技术措施对共享数据的机密性、完整性和可用性进行安全防护，如通过官网共享数据时，采取网页防篡改等技术，防范披露数据篡改风险；

c） 对数据共享全链路各环节的权限最小化控制，比如白名单控制并对异常进程监控；

d） 对数据共享全链路各环节风险进行监控；

h） 应采取必要的防泄漏技术或手段，防止工业数据在共享过程中发生泄露。

10.3 核心数据

原则上核心数据不允许共享。

11 工业数据开放

11.1 一般数据

一般数据开放安全防护要求如下：

a） 应对工业数据按照数据开放属性进行分类；

b） 对于分类属性为禁止开放的数据，不得开放；

c） 对于分类属性为受限开放、无条件开放的数据应满足以下要求：

1） 在开放前，对开放的必要性、范围、规模、方式等进行分析研判；

2） 数据安全管理责任部门应会同业务部门，对拟开放数据的合规性、业务需求、数据脱敏方案等进行审核与审批，业务部门应对开放渠道、开放时间、拟开放数据的真实性，以及数据脱敏效果进行确认；

3） 应采取合适方法对数据进行脱敏处理，保证工业数据开放安全；

4） 应确保工业数据开放内容的真实性、规范性、实效性和准确性。

11.2 重要数据

重要数据开放在 10.1 的基础上还应满足以下要求：

a） 应采取数据水印等必要措施保证工业数据开放安全；

b） 应在数据分类分级的基础上，建立工业数据开放管理制度，针对可对外公开和开放的数据进行开放前、开放中、开放后安全管理，具体包括开放前的数据内容、开放范围等审核，开放中对定期审查，以及开放后可能出现不良影响的应急处理机制；

c） 应制定工业数据开放审核制度，包括数据待开放内容、涉及的部门和组织、审核批准/否决、工业数据开放应急处理流程等，确保开放内容是可以公开并且符合法律法规要求的，工业数据开放的审核由工业数据开放安全管理部门负责，严格审核和管理开放的数据，确保已开放数据的合法性、真实性、准确性；

d） 应采取密码技术措施对开放数据的机密性、完整性和可用性进行安全防护，如通过官网开放数据时，采取包括网页防篡改等技术，防范披露数据篡改风险；

e） 对数据开放全链路各环节的权限最小化控制，如进行白名单控并对异常进程监控；

i） 应采取必要的防泄漏技术或手段，防止工业数据在开放过程中发生泄露。

11.3 核心数据

原则上核心数据不允许开放。

12 工业数据销毁

12.1 一般数据

一般数据销毁安全防护要求如下：

a） 应明确数据销毁对象、规则、流程技术等要求，对销毁活动进行记录和留存；

b） 工业企业客户删除业务应用数据时，工业互联网平台应将平台中的所有副本删除。

12.2 重要数据

重要数据销毁在 11.1 的基础上还应满足以下要求：

a） 应建立数据销毁审批机制，设置数据销毁相关监督角色、监督操作过程等；

b） 应采用多次擦写、消磁等技术手段，保证数据完全销毁，不留痕迹，不能恢复；

c） 应完全清除数据导入导出通道中的数据，并在数据存储空间被释放或重新分配前完全清除数据，防止数据被恶意恢复；

d） 应采取必要的防泄漏技术或手段，防止工业数据在销毁过程中发生泄露。

12.3 核心数据

核心数据销毁安全防护在 11.2 的基础上还应满足以下要求：

应采用粉碎、拆解等方式，实现物理销毁存储介质，并在保证数据完全删除后，再销毁废弃存储介

质，保证以不可逆的方式销毁数据。

13 工业数据出境

13.1 一般数据

一般数据出境应结合实际开展数据出境安全自评估和安全管理。自评估至少应包含以下几个方面：

a） 数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

b） 出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

c） 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

d） 数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

e） 与境外接收方拟订立的数据出境相关合同等法律文件是否充分约定了数据安全保护责任义务；

f） 其他可能影响数据出境安全的事项。

13.2 重要数据

重要数据出境在 12.1 的基础上还应满足以下要求：

a） 确需出境的，应依法依规进行数据出境安全评估；

b） 应具备数据出境安全监测能力，对通过评估的数据的出境行为、内容开展安全监测，加强数据出境安全风险防范和处置；

c） 应预留数据安全监测、检查等技术接口，为数据出境安全管理提供技术支持；

d） 应采取必要的防泄漏技术或手段，防止工业数据在出境过程中发生泄露。

13.3 核心数据

原则上核心数据不允许出境，确需出境的，应当依法依规进行数据出境安全评估。

14 工业数据转移

14.1 一般数据

一般数据转移应明确数据转移方案，并通过电话、短信、邮件、公告等方式通知受影响用户。

14.2 重要数据

重要数据转移在 13.1 的基础上还应满足以下要求：

a） 数据转移后，应在规定期限内向有关部门更新重要数据目录备案表；

b） 应采取必要的防泄漏技术或手段，防止工业数据在转移过程中发生泄露。

14.3 核心数据

核心数据转移在 13.2 的基础上还应满足以下要求：

应当评估安全风险，采取必要的安全保护措施，并报有关部门审查。

15 工业数据委托处理

15.1 一般数据

一般数据委托处理安全防护要求如下：

应通过签订合同协议等方式，明确数据安全保护要求和责任落实要求，规范数据使用权限、内容、范围及用途，对合作方数据使用情况进行监督管理。

15.2 重要数据

重要数据委托处理在 14.1 的基础上还应满足以下要求：

a） 应对被委托方的数据安全保护能力、资质进行评估或核实；

b） 应采取必要的防泄漏技术或手段，防止工业数据在委托处理过程中发生泄露。

15.3 核心数据

核心数据委托处理在 14.2 的基础上还应满足以下要求：

应当评估安全风险，采取必要的安全保护措施，并报有关部门审查。

参 考 文 献

[1] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

[2] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

[3] GB/T 41479-2022 信息安全技术 网络数据处理安全要求

[4] DB14/T 2526-2022 工业互联网综合平台 数据质量管理要求

[5] DB15/T 1874-2020 公共大数据安全管理指南

[6] DB15/T 2197-2021 大数据应用 数据安全管理责任指南

[7] DB21/T 3895-2023 工业数据流通 通用安全要求

[8] DB52/T 1557-2021 大数据开放共享安全管理规范