ICS XX.XXX

X XX

贵州省地方标准

DB 52/T XXXX.X-XXXXT

大数据开放共享交易安全管理规范

Security management specification for open sharing and

transaction of big data

（征求意见稿）

DB 52

201X-XX-XX发布 201X-XX-XX实施

贵州省市场监督管理局

发 布

目 录

[前 言 II](#_Toc4698096)

[1 范围 1](#_Toc4698097)

[2 规范性引用文件 1](#_Toc4698098)

[3 术语和定义 1](#_Toc4698099)

[4 原则和基本管理要求 2](#_Toc4698100)

[5 数据流通过程 5](#_Toc4698101)

[6 数据开放安全管理要求 6](#_Toc4698102)

[7 数据共享安全管理要求 9](#_Toc4698103)

前 言

本标准按照GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

**请注意：本文件的某些内容可能涉及专利内容。本文件的发布机构不承担识别这些专利的责任。**

本标准由贵州航天计量测试技术研究所提出。

本标准由贵州省大数据标准化技术委员会归口。

本标准起草单位：贵州航天计量测试技术研究所、贵州大学、贵州省机械电子产品质量监督检验院、贵州财经大学、贵州医科大学附属医院。

本标准主要起草人：潘积文、陈永久、杨玉龙、彭长根、丁红发、李明贵、禹忠、郑少波、杨大刚、朱义杰、李帅、冯迪、梁登辉。

大数据开放共享交易安全管理规范

# 1 范围

本标准规定了大数据开放共享的数据流通过程、安全管理原则和要求。

本标准适用于贵州省全省范围内政府、企事业单位、个人数据的开放共享安全管理。

# 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 35274-2017 信息安全技术 大数据服务安全能力要求

GB/T 35295-2017 信息技术 大数据 术语

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求

DB52/T 1123-2016 政府数据 数据分类分级指南

# 3 术语和定义

GB/T 35274-2017、GB/T 35295-2017界定的以及下列术语和定义适用于本文件。

3.1

数据开放 data open

由承担公共社会管理和服务职责的政府机构、企事业单位等公共机构产生、收集的所有信息，包括政务数据、交通数据、医疗数据等，仅承担社会责任的主体在授权范围内访问、咨询数据或用于科研、技术服务等。

3.2

数据共享 data share

承担社会责任的主体将自己掌控的数据在一定条件下与指定的第三方共享使用。

3.3

数据提供方 data provider

数据的拥有者，一般包括公共机构、企业、科学家、调研人员、从事数据搜索的工程师、网络运营商和末端用户，它将新的数据或信息引入数据流通平台。

3.4

数据接收方 data receiver

数据的使用者，一般包括末端用户、调研人员、应用和系统。

3.5

数据流通 data flow

数据流通主要是指数据开放、数据共享。

3.6

数据流通平台 data flow platform

用于数据流通的信息管理服务平台，包含承载数据的各业务系统。

3.7

数据流通服务机构 data circulation service institution

负责数据流通平台的日常管理、业务流转、运行维护等经营活动的组织机构，全权负责数据流通平台的管理。

3.8

数据流通安全管理机构 data circulation security management institution

负责数据流通服务机构的安全运营、数据流通平台及业务的安全管理等安全保障工作的组织机构，隶属于数据流通服务机构，全权负责数据流通服务机构的安全管理。

# 4 原则和基本管理要求

4.1 原则

4.1.1 职责明确

4.1.1.1 根据数据规模、数据重要性、组织规模等因素，组织应成立安全管理团队，安全管理团队为组织数据及使用安全负责。

4.1.1.2 组织应明确内部不同角色的数据安全管理职责。

4.1.1.3 组织应明确大数据生命周期中各项活动的实施主体及安全责任。

4.1.2 合法合规

4.1.2.1 组织应确保所有数据集和数据流的安全。

4.1.2.2 组织应正确处理个人信息、重要信息。

4.1.2.3 组织应实施合理的跨组织数据保留的策略和实践。

4.1.2.4 组织应理解数据相关的法律义务，并履行这些义务。

4.1.3 责任权属

4.1.3.1 当前控制数据的组织应对数据负责，当数据转移给其他组织时，责任不随数据转移而转移。

4.1.3.2 组织在数据转移前，应对数据进行风险评估，确保数据转移后的风险可承受，方可转移数据，并对数据转移给其他组织所造成的数据安全事件承担安全责任。

4.1.3.2 组织在数据转移前，应确保通过合同或其他诸如强制的内部策略等明确界定了接收方接收的数据范围和要求，确保其提供同等或更高的数据保护水平。

4.1.4 最小授权

4.1.4.1 在保证组织业务功能完整实现的基础上应赋予数据活动中各角色最小的操作权限，确保非法用户或异常操作所造成的损失最小。

4.1.4.2 所有角色应使用所授权范围内的数据，非授权范围内的数据使用应进行授权审批。

4.1.5 数据保护

涉及国家安全、公共利益、商业秘密和个人隐私的重要数据应得到充分保护。数据流通活动不应损害国家安全、公共利益和他人合法权益。数据清洗、加工、脱敏等流程应合规。数据流通中包含用户隐私数据的，应取得用户的同意。

4.1.6 安全审计

对数据进行修改、查询、导出、删除等操作时，组织应记录相应的操作，记录应可追溯可审查。

4.2 基本管理要求

4.2.1 安全管理策略

4.2.1.1 策略制定

数据流通服务机构应根据数据流通的安全需求和安全目标，结合自身的实际情况，制定明确的数据流通安全管理策略。

4.2.1.2 策略更新

数据流通服务机构应根据环境、平台和威胁的变化情况，及时调整现有的安全管理策略，制定新的防护计划，实施必要的防护措施，动态保障平台的安全性。

4.2.2 安全管理机构

4.2.2.1 数据流通服务机构基本要求

数据流通服务机构应满足以下要求：

1. 应为无违法违规记录的境内合法组织；
2. 应得到我国行政或主管部门的授权或许可；
3. 应具备承担数据流通服务相对应的安全保障能力；
4. 应将从事境内数据流通服务的数据流通平台部署在我国境内。

4.2.2.2 数据流通安全管理机构成立要求

数据流通安全管理机构成立应满足以下要求：

1. 应由数据流通服务机构主导成立；
2. 应由数据流通服务机构主管领导任责任人；
3. 应由信息化、业务工作、保卫和人事等有关部门人员共同组成，以组织协调整个机构的安全管理工作。

4.2.2.3 数据流通安全管理机构职责

数据流通安全管理机构应履行以下职责：

1. 组织、协调和指导数据流通服务机构的数据流通平台的建设、使用和维护开发工作；
2. 组织制定数据流通安全管理策略、工作流程和各种规章制度；
3. 组织对数据流通平台的安全检查和风险评估；
4. 审查和确定数据流通平台用户的职责和权限。

4.2.3 安全管理制度

4.2.3.1 安全责任制度

数据流通安全管理机构应建立相应的安全责任制度，明确岗位职责，实行领导责任制，层层落实，责任到人，使平台的每个工作人员都明确应承担的责任和义务。

4.2.3.2 安全工作制度

数据流通安全管理机构应在数据准备、流通磋商、流通实施、流通结束的全过程中，从人员、物理设施与环境、运行与开发、数据安全和个人信息安全保护等方面制定相应的安全工作制度。

# 5 数据流通过程

5.1 数据开放过程

数据开放是数据提供方、数据接收方对原始数据或加工处理后的数据依照既定开放过程进行的活动，数据开放服务参考框架如图1所示。数据开放涉及到数据提供方、数据接收方和数据流通服务机构。数据流通服务机构依托数据流通平台，为数据提供方、数据接收方提供数据开放服务。数据开放过程一般包括数据准备、数据发布和开放结束三个环节。



图 1 数据开放服务参考框架

5.2 数据共享过程

数据共享是数据提供方、数据接收方对原始数据或加工处理后的数据依照既定共享过程进行的活动。数据共享服务参考框架如图2所示。数据共享涉及到数据提供方、数据接收方和数据流通服务机构。数据流通服务机构依托数据流通平台，为数据提供方、数据接收方提供数据共享服务。数据共享过程一般包括数据准备、共享磋商、共享实施和共享结束四个环节。



图 2 数据共享服务参考框架

# 6 数据开放安全管理要求

6.1 数据准备

6.1.1 数据提供方要求

数据提供方应满足以下要求：

1. 应为无违法违规记录的境内合法组织或自然人；
2. 应完成在数据流通服务机构的注册，并经数据流通服务机构审核通过。

6.1.2 数据源安全

6.1.2.1 数据安全要求

数据流通安全管理机构应确保数据满足以下安全要求：

1. 应采用防计算机病毒系统对数据进行安全性扫描，确保数据的安全可靠；
2. 参与开放的数据应是真实可靠的数据，不应有蓄意伪造、篡改等造成数据污染行为；
3. 参与开放的数据不应携带涉密、商业秘密、隐私等敏感信息和谣言、反动言论等违法信息。

6.1.2.2 数据源平台安全

数据流通安全管理机构应确保数据源平台满足以下安全要求：

1. 应制定文档化的明确的平台安全性能检测策略；
2. 应采用国家相关主管部门批准使用的检测工具对平台进行安全性能检测，检测工具版本应及时更新；
3. 应对平台安全性能检测数据进行详细记录和分析，并对发现的漏洞和脆弱点及时修补。

6.1.2.3 数据分类要求

应依据DB52/T 1123-2016等相关文件对开放的数据进行分类，数据分类应满足以下要求：

a) 数据分类应易于理解；

b) 应形成文档化的数据分类条目，便于查询。

6.1.3 访问控制策略

6.1.3.1 策略制定

数据流通服务机构应根据数据提供方数据开放的需求和目标，结合数据接收方的实际需求，按照最小授权原则，制定明确的数据开放访问控制策略。

6.1.3.2 策略更新

数据流通服务机构应根据数据提供方数据开放的需求和目标、数据接收方的需求、数据流通平台的变化情况，及时调整现有的访问控制策略，动态保障数据流通平台的访问权限。

6.1.4 方案设计要求

数据流通服务机构应在归口行政管理部门的指导与监督下，按照GB/T 25070的要求，选择具有相应能力的承建单位承担或参与数据开放方案的设计，方案设计应满足以下要求：

1. 方案设计前应经过安全性及隐私泄露风险评估，根据评估结果确定应采取的保护措施；
2. 应选择具有相应能力的承建单位承担或参与数据开放方案的设计；
3. 数据流通服务机构应联合数据提供方对设计方案进行审查论证，归口行政管理部门应参与方案审查论证，在整体安全性方面加强指导，严格把关。

6.2 数据发布安全

6.2.1 数据流通平台安全

应根据信息安全等级保护要求，具体依据GB/T 22239和GB/T 25070中的相应要求，对数据流通平台的安全性作如下要求：

1. 应定期对数据流通平台进行安全性能检测；
2. 应制定文档化的明确的平台安全性能检测策略；
3. 应采用国家相关主管部门批准使用的检测工具对平台进行安全性能检测，检测工具版本应及时更新；
4. 应对平台安全性能检测数据进行详细记录和分析，并对发现的漏洞和脆弱点及时修补。

6.2.2 数据传输安全

数据传输应满足以下安全要求：

1. 应对数据接收方身份进行鉴别和认证；
2. 应采用密码技术进行数据保护，密码技术应采用国产密码算法。

6.2.3 数据完整性保护

应根据信息安全等级保护要求，具体依据GB/T 22239和GB/T 25070中的相应要求，对数据发布中的数据完整性作如下要求：

1. 应制定文档化的明确的数据完整性保护策略；
2. 应对平台中传输的数据进行完整性检测，及时发现数据被篡改、删除、插入的情况，并生成审计日志。

6.2.4 数据安全审计

数据开放过程应满足以下安全审计要求：

1. 应制定文档化的明确的数据发布安全审计策略，策略应根据数据发布的变化情况动态更新；
2. 安全审计应与数据源安全、访问控制等安全功能的设计紧密结合，针对数据开放过程中的可审计事件产生审计记录；
3. 审计记录应包括以下内容：数间发生的时间、地点、类型、主体、客体和结果（成功或失败）；
4. 应对已存储的审计记录进行保护，能检测或防止对审计记录的修改和伪造；
5. 审计记录应长期保存；
6. 应定期对审计记录进行审查或分析，调查可疑行为及违规操作，采取相应的措施，并及时报告。

6.2.5 数据权属明确

数据开放过程中，应明确数据权属不变，仍为数据提供方所有，数据转移过程中应遵循责任权属原则。

6.3 开放结束

6.3.1 数据接收方要求

数据接收方应满足以下要求：

1. 应为无违法违规记录的境内合法组织或自然人；
2. 应完成在数据流通服务机构的注册，并经数据流通服务机构审核通过；
3. 应证明其具备对开放数据实施安全保护的能力；
4. 应提供书面的数据开放和使用安全承诺，内容包括但不限于：遵守数据开放安全原则、愿意接受数据流通服务机构安全监督、遵守数据提供方提出的数据安全要求、对所持有数据提供充分的安全保护、未经明确授权不公开或转交数据给第三方、未经明确授权不应转移或携带数据出境等；
5. 在按照数据开放约定方式完成数据使用后，应及时销毁开放数据；
6. 数据流通服务机构应建立和执行针对数据接收方的安全监管制度和流程。

6.3.2 数据销毁要求

数据销毁应满足以下要求：

1. 数据流通平台在按照数据开放约定方式完成数据开放后，应及时销毁开放数据；
2. 数据流通平台应长期保留数据流通日志记录，以备数据溯源；
3. 数据流通平台应长期保留已流通数据的数据水印，以备数据溯源；
4. 数据流通安全管理机构应建立和执行针对数据销毁的安全监管制度和流程。

# 7 数据共享安全管理要求

7.1 数据准备

7.1.1 数据提供方要求

数据提供方应满足以下要求：

1. 应为无违法违规记录的境内合法组织或自然人；
2. 应完成在数据流通服务机构的注册，并经数据流通服务机构审核通过。

7.1.2 数据源安全

7.1.2.1 数据安全要求

数据流通安全管理机构应确保数据满足以下安全要求：

1. 应采用防计算机病毒系统对数据进行安全性扫描，确保数据的安全可靠；
2. 参与共享的数据应当是真实可靠的数据，不应有蓄意伪造、篡改等造成数据污染行为；
3. 参与共享的数据不应携带涉密、商业秘密、隐私等敏感信息和谣言、反动言论等违法信息。

7.1.2.2 数据源平台安全

数据流通安全管理机构应确保数据源平台满足以下安全要求：

1. 应制定文档化的明确的平台安全性能检测策略；
2. 应采用国家相关主管部门批准使用的检测工具对平台进行安全性能检测，检测工具版本应及时更新；
3. 应对平台安全性能检测数据进行详细记录和分析，并对发现的漏洞和脆弱点及时修补。

7.1.2.3 数据分类要求

应依据DB52/T 1123-2016等相关文件对共享的数据进行分类，数据分类应满足以下要求：

a) 数据分类应易于理解；

b) 应形成文档化的数据分类条目，便于查询。

7.1.3 访问控制策略

7.1.3.1 策略制定

数据流通服务机构应根据数据提供方数据共享的需求和目标，结合数据接收方的实际需求，按照最小授权原则，制定明确的数据共享访问控制策略。

7.1.3.2 策略更新

数据流通服务机构应根据数据提供方数据共享的需求和目标、数据接收方的需求、数据流通平台的变化情况，及时调整现有的访问控制策略，动态保障数据流通平台的访问权限。

7.1.4 方案设计要求

数据流通服务机构应在归口行政管理部门的指导与监督下，按照GB/T 25070的要求，选择具有相应能力的承建单位承担或参与数据共享方案的设计，方案设计应满足以下要求：

1. 方案设计前应经过风险评估，根据评估结果确定应采取的保护措施；
2. 应选择具有相应能力的承建单位承担或参与数据共享方案的设计；
3. 数据流通服务机构应联合数据提供方对设计方案进行审查论证，归口行政管理部门应当参与方案审查论证，在整体安全性方面加强指导，严格把关。

7.2 数据共享磋商

7.2.1 共享磋商要求

数据共享磋商应满足以下要求：

1. 数据提供方、数据接收方应对共享数据的用途、使用范围、共享方式和使用期限等协商和约定，形成共享合同；
2. 数据流通服务机构应对共享合同从数据流通安全、个人信息保护安全等方面进行审核，确保符合相关法律法规和标准等合规性要求，撤销不符合要求的共享合同；
3. 数据流通服务机构应对审核通过的合同进行登记备案，并对数据提供方、数据接收方发出合同确认通知。

7.2.2 数据共享承诺

数据共享承诺应满足以下要求：

1. 数据提供方、数据流通服务机构、数据接收者在启动数据共享流程前应签订书面的数据共享和使用安全承诺；
2. 安全承诺内容包括但不限于：遵守数据共享安全原则、数据流通服务机构愿意接受数据提供方的安全监督、数据接收方愿意接受数据流通服务机构安全监督、遵守数据提供方提出的数据安全要求、对所持有数据提供充分的安全保护、未经明确授权不公开或转交数据给第三方、未经明确授权不应转移或携带数据出境等。

7.3 数据共享安全

7.3.1 数据流通平台安全

应根据信息安全等级保护要求，具体依据GB/T 22239和GB/T 25070中的相应要求，对数据流通平台的安全性作如下要求：

1. 应定期对数据流通平台进行安全性能检测；
2. 应制定文档化的明确的平台安全性能检测策略；
3. 应采用国家相关主管部门批准使用的检测工具对平台进行安全性能检测，检测工具版本应及时更新；
4. 应对平台安全性能检测数据进行详细记录和分析，并对发现的漏洞和脆弱点及时修补。

7.3.2 数据传输安全

数据传输应满足以下安全要求：

1. 应对数据提供方、数据接收方身份进行鉴别和认证。
2. 应采用密码技术进行数据保护，密码技术应采用国产密码算法。

7.3.3 数据完整性保护

应根据信息安全等级保护要求，具体依据GB/T 22239和GB/T 25070中的相应要求，对数据共享中的数据完整性作如下要求：

1. 应制定文档化的明确的数据完整性保护策略；
2. 应对平台中传输的数据进行完整性检测，及时发现数据被篡改、删除、插入的情况，并生成审计日志。

7.3.4 数据安全审计

数据共享过程应满足以下安全审计要求：

1. 应制定文档化的明确的数据共享安全审计策略，策略应根据数据发布的变化情况动态更新；
2. 安全审计应与数据源安全、访问控制等安全功能的设计紧密结合，针对数据共享过程中的可审计事件产生审计记录；
3. 审计记录应包括以下内容：数间发生的时间、地点、类型、主体、客体和结果（成功或失败）；
4. 应对已存储的审计记录进行保护，能检测或防止对审计记录的修改和伪造；
5. 审计记录应长期保存；
6. 应定期对审计记录进行审查或分析，调查可疑行为及违规操作，采取相应的措施，并及时报告。

7.3.5 数据权属明确

数据共享过程中，应明确数据权属不变，仍为数据提供方所有，数据转移过程中应遵循责任权属原则。

7.4 共享结束

7.4.1 数据接收方要求

数据接收方应满足以下要求：

1. 应为无违法违规记录的境内合法组织或自然人；
2. 应完成在数据流通服务机构的注册，并经数据流通服务机构审核通过；
3. 应证明其具备对共享数据实施安全保护的能力；
4. 在按照数据共享约定方式完成数据使用后，应及时销毁共享数据；
5. 数据流通服务机构应建立和执行针对数据接收方的安全监管制度和流程。

7.4.2 数据销毁要求

数据销毁应满足以下要求：

1. 数据流通平台在按照数据共享约定方式完成数据共享后，应及时销毁共享数据；
2. 数据流通平台应长期保留数据流通日志记录，以备数据溯源；
3. 数据流通平台应长期保留已流通数据的数据水印，以备数据溯源；
4. 数据流通安全管理机构应建立和执行针对数据销毁的安全监管制度和流程。