ICS 35.240.70
CCS L 70

DB51

四 川 省 地 方 标 准

DB51/T 3056—2023

政务数据 数据分类分级指南

Government affairs data
guide for data categorization and classification

2023－04－28 发布　　2023－06－01 实施

四川省市场监督管理局　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。

本文件由四川省大数据中心提出、归口并解释。

本文件起草单位：四川省大数据中心、北京启明星辰信息安全技术有限公司、信息产业电子第十一设计研究院科技工程股份有限公司、中国电子系统技术有限公司、浪潮云信息技术股份公司。

本文件主要起草人：赵启斌、任轲正、齐翌、杨颋、刘冰、卢彬、刘雯、吴晓蓉、余东亮、黄健、孙光春、张铭宇、杨燕、吴凤、尹嘉奇、周奕含、雷蕾、蒋晓、刘艳慧、刘宏、曾刚、朱孟凯、王燕、伏晓龙。

本文件为首次发布。

政务数据 数据分类分级指南

1 范围

本文件规定了四川省范围内政务数据资源管理过程中政务数据分类分级的术语和定义、数据分类、数据分级等要求。

本文件适用于指导四川省范围内政务数据的分类分级工作。

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 25069-2022 信息安全技术 术语

GB/T 38664.1-2020 信息技术 大数据 政务数据开放共享 第1部分：总则

GB/T 38667-2020 信息技术 大数据 数据分类指南

GB/T 39477-2020 信息安全技术 政务信息共享 数据安全技术要求

DB51/T 2847-2021 四川省政务信息资源目录编制指南

3 术语和定义

GB/T 25069-2022、GB/T 38664.1-2020、GB/T 39477-2020、GB/T 38667-2020界定的以及下列术语和定义适用于本文件。

3.1

政务数据 government affairs data

各级政务部门及其技术支撑单位在履行职责过程中依法采集、生成、存储、管理的各类数据资源。

注：根据可传播范围，政务数据一般包括可共享政务数据，可开放政务数据及不宜开放共享政务数据。

[来源：GB/T 38664.1-2020，定义3.1，有修改]

3.2

敏感数据 sensitive data

由权威机构确定的受保护的信息数据。

注：敏感信息数据的泄露、修改、破坏或丢失会对人或事产生可预知的损害。

[来源：GB/T 39477-2020，定义3.7]

3.3

政务数据分类 government affairs data categorization

将具有同一属性或特征的政务数据，按照一定的原则和方法进行归类和区分，建立起一定的分类体系和排列顺序。

[来源：GB/T 38667-2020，定义3.3，有修改]

3.4

政务数据分级 government affairs data classification

根据政务数据的敏感程度和被破坏后对受影响对象的影响程度，按照一定的原则和方法进行定级，为政务数据全生命周期过程中的安全管理和策略制定提供支撑。

3.5

政务数据共享 government affairs data sharing

各级政务部门因履行职责需要，使用其他政务部门的政务数据以及为其他政务部门提供政务数据的行为。

[来源：GB/T 38664.1-2020，定义3.2]

3.6

政务数据开放 government affairs data opening

政务部门在安全保密、公共利益导向前提下，面向公民、法人和其他组织以非排他形式依法提供政务数据的行为。

[来源：GB/T 38664.1-2020，定义3.3，有修改]

4 数据分类

4.1 分类原则

4.1.1 科学性

以政务数据多维特征及其各政务数据之间的逻辑关联为基础，依据数据的本质和内在规律进行科学系统化分类。

4.1.2 实用性

政务数据分类应从基础库建设及政务数据应用等实际需求出发，确保各个类目下都含有真实的有价值数据，不设定无价值类目，设定的数据类目符合普遍认知且综合实用。

4.1.3 稳定性

选择政务数据分类最稳定、最本质的特征指标和属性指标，一经分类生效，便应在一定时期内保持分类相对地稳定不变。

4.1.4 扩展性

政务数据分类保证类目的可扩展性、兼容性，可适应未来阶段政府部门机构调整、经济发展变化、基础库建设规划调整导致的类目增减和数据类型变化等情况。

4.2 分类要素

4.2.1 资源属性

按资源属性将数据分为基础信息资源、主题信息资源、部门信息资源三种类型。

——基础信息资源主要是参考DB51/T 2847-2021，对基础信息的分类，包括人口基础信息资源、法人单位基础信息资源、自然资源和空间地理基础信息资源、社会信用基础信息资源、电子证照基础信息资源等。

——主题信息资源参考DB51/T 2847-2021，对围绕经济社会发展的同一主题领域的数据进行分类，包括但不限于公共服务、健康保障、社会保障、食品安全、药品安全、安全生产、价格监管、金融监管、能源安全、信用体系、城乡建设、社区治理、生态环保、应急维稳等。

——部门信息资源参考DB51/T 2847-2021，按照部门所属性质进行分类，包括各级地方党委、人大、政府、政协、法院、检察院及其直属各部门（单位）等的信息资源。

4.2.2 共享属性

依据《政务信息资源共享管理暂行办法》（国发〔2016〕51号）中政务信息资源共享属性，将政务数据分为无条件共享类、有条件共享类、不予共享类三类（共享属性与数据安全等级对应参考原则见附录B数据共享、开放与安全级别的对应关系）。

——无条件共享类：可提供给所有政务部门共享使用的政务数据属于无条件共享类。

——有条件共享类：可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用的政务数据属于有条件共享类。

——不予共享类：不宜提供给其他政务部门共享使用的政务数据属于不予共享类。

4.2.3 开放属性

政务数据的开放属性参考DB51/T 2847-2021中元数据描述的开放属性为标准，将政务数据开放类型分为无条件开放类、有条件开放类和不予开放类三类（开放属性与数据安全等级对应参考原则见附录B数据共享、开放与安全级别的对应关系）。

——无条件开放类：可提供给所有自然人、法人和非法人组织使用的政务数据属于无条件开放类。

——有条件开放类：可提供给部分自然人、法人和非法人组织使用或仅能够部分提供给所有自然人、法人和非法人组织开放使用的政务数据属于有条件开放类。

——不予开放类：不宜提供给任何自然人、法人和非法人组织开放使用的政务数据属于不予开放类。

4.3 分类步骤

4.3.1 概述

分类流程包括分类准备、分类判定、分类审批、分类实施及结果核查。

4.3.2 分类准备

4.3.2.1 分类准备包括调研数据现状、确定分类对象、选择分类要素。

4.3.2.2 调研数据现状指对数据的产生情况、存储现状、质量情况、业务类型、敏感程度、应用情况、时效性情况以及权属情况等进行调查研究。

4.3.2.3 确定分类对象是对包括但不限于数据分类业务场景、产生的起止时间、数据量大小、存储方式、产生来源等的梳理。

4.3.2.4 选择分类要素需结合自身实际按数据属性维度来选择。

注：分类要素详见第4.2节。

4.3.3 分类判定

按照实际业务情况，从实际需求出发，对数据的资源属性分类维度、共享属性分类维度及开放属性分类维度分别进行分类判定。其中资源属性分类维度中的三个类别需同时进行判定和选择；共享属

性分类维度及开放属性分类维度这两种维度中的分类类别需分别选择一个。在确保数据三个属性维度的类别均已确认后，输出数据分类表。

4.3.4 分类审批

审核数据分类的对象、方法及分类表，并对数据分类对象、方法及分类表进行审议批准。

4.3.5 分类实施

结合政务数据的实际应用场景拟定具体的分类实施流程，并使用自动化开发工具或脚本，利用其分类算法对政务数据进行分类。同时记录分类实施过程中的各个步骤及其分类结果。

4.3.6 结果核查

根据实际数据的应用场景，核查验证分类结果及实施过程是否合规，包括但不限于数据分类表、分类过程记录、分类方法内容的核查。

5 数据分级

5.1 分级原则

5.1.1 明确场景

政务数据分级要充分参考各类数据应用场景，保证政务数据分级的可行性、实用性。

5.1.2 科学定级

政务数据分级按照数据资源的多维特征及其之间存在的逻辑关联关系进行系统化、标准化分级，保证政务数据级别的准确性、客观性。

5.1.3 自主定级

按照本文件分级方法，对各类政务数据进行自主分级。

5.2 分级要素

5.2.1 影响对象

依照《中华人民共和国数据安全法》要求，数据分级应该充分考虑中华人民共和国国家安全、公共利益或者公民、组织合法权益，并结合四川省政务数据的实际情况，四川省政务数据分级需要考虑的影响对象包括以下四个：

——对国家安全的影响。一般指数据发生泄露、篡改、丢失或滥用后，可能对国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益、保障持续安全状态的能力造成影响。

——对社会秩序及公共利益的影响。一般指数据发生泄露、篡改、丢失或滥用后，可能对社会的医疗卫生、生产经营、教学科研、公共环境、市政项目、文体旅游、社会福利、住宅用房及其他公用事业等社会秩序和公众的身心健康、政治权利、人身自由、经济权益等造成影响。

——对政府机构、企事业单位及其他社会组织自身权益的影响。一般指数据发生泄露、篡改、丢失或滥用后，可能对某政府机构、企事业单位或其他社会组织的生产经营、声誉形象、公信力、资金资产等造成影响。

——对个人权益的影响。一般指数据发生泄露、篡改、丢失或滥用后，可能对个人隐私、个人财产、生命安全、精神、名誉、私人活动和领域等造成影响。

5.2.2 影响程度

影响程度应充分考虑对影响对象的范围、是否可控以及影响所造成的损害程度来进行判别，判别的参考依据如表1所示。

表1 影响程度判别参考依据

程度	定义
轻微影响	数据发生泄露、篡改、丢失或滥用后对影响对象等的运行、资产、安全及合法权益造成轻微损害或一般损害，范围较小、程度可控，结果可以补救。
中等影响	数据发生泄露、篡改、丢失或滥用后对影响对象等的运行、资产、安全及合法权益造成较为严重的损害，范围较大、程度可控、结果可以补救或范围较小但结果不可逆但可以采取措施降低损失。
严重影响	数据发生泄露、篡改、丢失或滥用后对影响对象等的运行、资产、安全及合法权益造成严重损害，影响的范围、程度不可控且结果不可逆。

5.3 分级方法

根据数据的安全属性破坏后的影响对象、影响程度，将数据划分为四级，触发其中一个影响对象即达到对应的最低安全等级，如表2所示。其中以共享属性和开放属性进行分类的数据与分级级别之间的关系可参考附录B。

表2 分级方法

最低安全等级	敏感级别	影响对象	影响程度	数据特性
一级	非敏感级	国家安全	无影响	1.原则可提供给所有政务部门共享使用并面向社会完全开放或脱敏后开放。 2.数据发生泄露、篡改、丢失或滥用后，对个人权益、政府机构、企事业单位及其他社会组织的正常运作及合法权益不造成影响或影响微弱可以忽略；对社会秩序、公共利益以及国家安全不造成影响。
		社会秩序及公共利益	无影响	
		政府机构、企事业单位及其他社会组织	无影响	
		个人权益	无影响	
二级	低敏感级	国家安全	无影响	1.数据可进行有条件共享和开放。可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用；可提供给部分或部分提供给个人和组织使用。 2.数据发生泄露、篡改、丢失或滥用后，对个人权益、政府机构、企事业单位及其他社会组织的正常运作及合法权益造成轻微影响；对社会秩序及公共利益、国家安全不造成影响。
		社会秩序及公共利益	无影响	
		政府机构、企事业单位及其他社会组织	轻微影响	
		个人权益	轻微影响	

表 2（续）

最低安全等级	敏感级别	影响对象	影响程度	数据特性
三级	敏感级	国家安全	无影响	1.数据可进行有条件共享和开放。可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用；可提供给部分或部分提供给个人和组织开放使用。 2.数据发生泄露、篡改、丢失或滥用后，对个人权益、政府机构、企事业单位及其他社会组织的正常运作和合法权益造成中等影响；对社会秩序及公共利益造成轻微影响；对国家安全不造成影响。
		社会秩序及公共利益	轻微影响	
		政府机构、企事业单位及其他社会组织	中等影响	
		个人权益	中等影响	
四级	极敏感级	国家安全	轻微影响/中等影响/严重影响	1.数据一般不可被共享和开放，或可通过申请向特定单位或人员公开。 2.数据发生泄露、篡改、丢失或滥用后，对个人权益、政府机构、企事业单位及其他社会组织造成严重影响；对社会秩序及公共利益造成中等及以上影响；对国家安全造成影响。
		社会秩序及公共利益	中等影响/严重影响	
		政府机构、企事业单位及其他社会组织	严重影响	
		个人权益	严重影响	

5.4 分级步骤

5.4.1 概述

分级流程包括分级准备、分级判定、分级审批、分级实施及结果核查。

5.4.2 分级准备

对照现行相关法律法规、规章制度及行业相关政策进行分级工作，并识别数据安全定级关键要素。

5.4.3 分级判定

根据数据的安全属性破坏后的影响对象、影响程度进行数据的分级，并输出数据分级表。
具体的分级方法可参考5.2节及5.3节。

5.4.4 分级审批

审核数据分级的结果，并对数据分级结果进行审议批准。

5.4.5 分级实施

拟定具体的分级实施流程，并使用自动化开发工具或脚本，利用其分级算法对政务数据进行分级。同时记录分级实施过程中的各个步骤及其分级结果。

5.4.6 结果核查

核查验证分级结果及实施过程是否合规，包括但不限于分级判定及分级过程记录的核查。

附 录 A
（资料性）
数据分级判定及判例参考

A.1　数据集名称：失信被执行人信息表。

A.2　数据项：失信被执行人行为具体情形、被执行人的履行情况、生效法律文书确定的义务、做出执行依据单位、立案时间、执行依据文号、执行法院、案号、身份证号码、姓名、性别、年龄。

A.3　首先对整个数据集进行分析，失信被执行人信息按照类别属于司法信息，但包含个人信息在内，失信被执行人信息按照相关法律要求，应该向社会公开；而个人信息，如身份证号属于个人隐私数据，在本数据集中，身份证号发生数据泄露、篡改、丢失或滥用后对较大范围自然人的个人隐私、财产、生命安全、精神、名誉、私人活动和领域等造成中等影响，不宜或应有条件向社会公开或向其他机构进行共享。因此得出该数据集最高级别可定位为三级。

A.4　对于本数据集的数据项分析及数据级别判定标准如表 A.1 所示。

表A.1 数据项级别判定示例

数据项	数据分析	数据级别
失信被执行人行为具体情形	依据法律法规规定需要公开数据	一级
被执行人的履行情况	依据法律法规规定需要公开数据	一级
生效法律文书确定的义务	依据法律法规规定需要公开数据	一级
做出执行依据单位	依据法律法规规定需要公开数据	一级
立案时间	依据法律法规规定需要公开数据	一级
执行依据文号	依据法律法规规定需要公开数据	一级
执行法院	依据法律法规规定需要公开数据	一级
案号	依据法律法规规定需要公开数据	一级
身份证号码	个人隐私数据	三级
姓名	依据法律法规规定需要公开数据	一级
性别	依据法律法规规定需要公开数据	一级
年龄	依据法律法规规定需要公开数据	一级

附 录 B
（资料性）
数据共享、开放与安全级别的对应关系

依据《政务信息资源共享管理暂行办法》（国发〔2016〕51号）遵照政务数据资源以共享为原则，不共享为例外；政务数据资源开放应当遵循需求导向、分类分级、便捷高效、安全可控等政务数据共享和开放的原则，与数据等级进行一一对应，参考标准如表B.1。

表B.1 数据等级及共享开放对应参考原则

数据等级	共享	开放
一级	**无条件共享** （原则上无条件共享，可提供给所有政务部门共享使用。如列为有条件共享，应当有法律、行政法规的规定或者相关政策为依据。）	**无条件开放** （原则上在不违反法律法规的条件下，面向社会完全开放或脱敏后开放。）
二级	**有条件共享** （原则上有条件共享，可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用。如列为不予共享，应当有法律、行政法规的规定或者相关政策为依据。）	**有条件开放** （可提供给部分自然人、法人和非法人组织使用，仅能够部分提供给所有自然人、法人和非法人组织开放使用或在不违反法律法规的条件下，面向社会脱敏后有条件开放。）
三级		
四级	**不予共享/有条件共享** （原则上不予共享，不宜提供给其他政务部门共享使用，或提供可用不可见的有条件共享。）	**不予开放/有条件开放** （不宜提供给任何自然人、法人和非法人组织开放使用，原则上不予开放，或在不违反法律法规的条件下提供可用不可见的有条件开放。）

附 录 C
（资料性）
安全级别变更场景及原则

导致数据发生升降级的主要技术手段有数据脱敏、删除关键字段、汇聚融合等，下表为数据安全级别升降级措施。数据安全升降级原则上只进行相邻数据级别的升降，在需跨多级升降数据安全级别的场景，应按照逐级升降的原则进行。

表C.1 数据安全级别升降级措施

数据安全级别	措施
1级→2级	汇聚融合
2级→1级	脱敏
2级→3级	汇聚融合，特定时间或事件后信息具有敏感性
3级→2级	脱敏，删除非公开信息，特定时间或事件后信息失去原有敏感性
3级→4级	汇聚融合，特定机构特定时间或事件后信息具有高安全等级
4级→3级	脱敏，从数据中删除能够直接获取到个人信息主体及机密内容，特定时间或事件后信息失去原有敏感性

附 录 D
（资料性）
数据分级保护措施

数据分级后，应按照相应的保护措施，对数据进行分级保护。数据分级保护措施如表D.1所示。

表D.1 数据分级保护措施

政务数据管理活动及流程	保护措施	数据分级保护措施示例			
		一级	二级	三级	四级
数据采集	管理保护措施	1.明确数据安全管理要求及数据采集目的、用途、范围。 2.明确数据采集来源、采集渠道，对数据提供方及被采集对象的数据提供合法性和正当性的确认。	1.明确数据安全管理要求及数据采集目的、用途、范围。 2.明确数据采集来源、采集渠道，对数据提供方及被采集对象的数据提供合法性和正当性的确认。 3.建议建立数据采集及风险评估流程，确保数据采集流程的一致性及采集授权、采集过程的详细可见。 4.建议建立数据源管理制度，保证采集来源识别、管理及采集数据的可追溯性管理。	1.明确数据安全管理要求及数据采集目的、用途、范围。 2.明确数据采集来源、采集渠道，对数据提供方及被采集对象的数据提供合法性和正当性的确认。 3.建立数据采集及风险评估流程，确保数据采集流程的一致性及采集授权、采集过程的详细可见。 4.建立数据源管理制度，保证采集来源识别、管理及采集数据的可追溯性管理。	1.明确数据安全管理要求，具备完整的采集审核机制，经过相关主管领导审核确认，明确数据采集目的、用途、范围。 2.明确数据采集来源、采集渠道，对数据提供方及被采集对象的数据提供合法性和正当性的确认。 3.建立数据采集及风险评估流程，确保数据采集流程的一致性及采集授权、采集过程的详细可见。 4.建立数据源管理制度，保证采集来源识别、管理及采集数据的可追溯性管理。
	技术保护措施	1.针对数据采集过程执行有效的日志记录。	1.建议建立数据采集过程数据保护机制，明确数据采集过程中的个人信息和重要数据的安全控制措施。 2.建议部署统一化数据采集工具，设定安全策略。 3.针对采集源进行识别和记录的相关技术及工具，确保数据源可追溯。 4.建议针对数据采集过程执行有效的日志记录。	1.建立数据采集过程数据保护机制，明确数据采集过程中的个人信息和重要数据的安全控制措施。 2.部署统一化数据采集工具，设定安全策略。 3.针对采集源进行识别和记录的相关技术及工具，确保数据源可追溯，并对数据来源进行合法性确认。 4.针对数据采集过程执行有效的日志记录。 5.实施数据采集过程中的数据防泄漏技术。	1.建立数据采集过程数据保护机制，明确数据采集过程中的个人信息和重要数据的安全控制措施。 2.部署统一化数据采集工具，设定安全策略。 3.针对采集源进行识别和记录的相关技术及工具，确保数据源可追溯，并对数据来源进行合法性确认。 4.针对数据采集过程执行有效的日志记录。 5.实施数据采集过程中的数据防泄漏技术。 6.通过经认证或可信的传输通道采集数据。

表D.1（续1）

政务数据管理活动及流程	保护措施	数据分级保护措施示例			
		一级	二级	三级	四级
数据传输	管理保护措施	/	1.明确政务数据加密传输场景。	1.明确政务数据加密传输场景。 2.明确加密设备或工具所约定的加密算法要求要求。	1.明确政务数据加密传输场景。 2.明确加密设备或工具所约定的加密算法要求和密钥管理要求。
	技术保护措施	/	1.建立安全的数据传输通道。 2.建立政务数据加密传输机制。	1.建立安全的数据传输通道。 2.对传输通道两端的主体身份进行鉴别与认证。 3.建立政务数据加密传输机制。 4.确保网络的高可用性。	1.建立安全的数据传输通道。 2.对传输通道两端的主体身份进行鉴别与认证。 3.建立政务数据加密传输机制。 4.确保网络的高可用性。 5.具备相对完整的密钥生命周期管理。
数据存储	管理保护措施	1.建议制定存储系统建立安全管理规范。	1.建议制定存储系统建立安全管理规范和操作流程规范。	1.对存储系统制定安全管理规范和操作流程规范。 2.对存储系统的账号、权限、日志、加密按照统一要求进行管理。	1.对存储系统制定安全管理规范和操作流程规范。 2.对存储系统的账号、权限、日志、加密按照统一要求进行管理。 3.建立物理存储介质和逻辑存储安全管理制度。
	技术保护措施	1.建立数据备份机制。	1.建立存储系统操作日志采集机制，定期识别账号确权。 2.建立数据备份机制。	1.建立对重要数据存储系统及其安全配置定期扫描，符合系统安全基线要求。 2.建立存储系统操作日志采集机制，定期识别账号确权。 3.建立数据备份机制。 4.对离线环境进行存储加密。	1.建立对重要数据存储系统及其安全配置定期扫描，符合系统安全基线要求。 2.建立存储系统操作日志采集机制，定期识别账号确权。 3.建立本地和异地双向数据备份机制。 4.进行加密存储。

表D.1（续2）

政务数据管理活动及流程	保护措施	数据分级保护措施示例			
		一级	二级	三级	四级
数据处理	管理保护措施	1.具备数据分析和使用过程中的日志记录工具，并对分析过程和结果进行安全审查，确定使用授权流程。	1.建议明确严格的统一化访问控制管理要求、用户和内容的权限。	1.明确严格的统一化访问控制管理要求，建立用户和内容的权限。 2.建立统一的数据脱敏制度规范和流程。 3.制定数据分析过程中数据资源操作规范和实施指导。 4.制定数据权限管理和使用者安全责任制度。	1.明确严格的统一化访问控制管理要求，建立用户和内容的权限。 2.建立统一的数据脱敏制度规范和流程。 3.制定数据分析过程中数据资源操作规范和实施指导。 4.制定数据权限管理和使用者安全责任制度。 5.建立数据分析结果的风险评估机制。
	技术保护措施	/	1.应对用户进行身份鉴别。 2.采用数据分析和使用过程中的日志记录工具，并对分析过程和结果进行安全审查，确定使用授权流程。 3.应使用相关技术手段对数据处理过程进行全程监控，必要时进行操作阻断。	1.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。 2.应采用数据静态脱敏和数据动态脱敏能力的工具，并对脱敏操作过程留存日志记录。 3.应采用数据分析和使用过程中的日志记录工具，并对分析过程和结果进行安全审查，确定使用授权流程。 4.应使用相关技术手段对数据处理过程进行全程监控，必要时进行操作阻断。	1.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。 2.应采用数据静态脱敏和数据动态脱敏能力的工具，并对脱敏操作过程留存日志记录。 3.应采用数据分析和使用过程中的日志记录工具，并对分析过程和结果进行安全审查，确定使用授权流程。 4.应使用相关技术手段对数据处理过程进行全程监控，必要时进行操作阻断。 5.应使用对个人身份信息、重要或敏感数据进行处理操作的日志记录工具。

表D.1（续3）

政务数据管理活动及流程	保护措施	数据分级保护措施示例			
		一级	二级	三级	四级
数据共享	管理保护措施	1.制定数据共享目录，明确数据共享涉及的相关机构和部门相关职责和权限，明确相关保护责任。	1.制定数据共享目录，明确数据共享涉及的相关机构和部门相关职责和权限，明确相关保护责任。 2.建立政务数据共享的审核流程，对数据的使用申请进行严格审批和授权。	1.制定数据共享目录，明确数据共享涉及的相关机构和部门相关职责和权限，明确相关保护责任。 2.建立常见共享场景的细化规划要求，指导数据共享场景的风险把控。 3.建立规范性政务数据共享的审核流程，对共享数据的试用申请进行严格审批和授权。	/
	技术保护措施	/	1.建立数据共享唯一通道，并进行严格审核及详细记录。 2.采用数据共享过程监控及数据共享审计措施，确保数据共享未超过授权范围。	1.建立数据共享唯一通道，并进行严格审核及详细记录。 2.采用数据共享过程监控及数据共享审计措施，确保数据共享未超过授权范围。 3.数据共享前进行对应脱敏降级处理。	/
数据开放	管理保护措施	1.建议在对外开放过程中建立开放数据审批流程。	1.建立数据开放发布管理制度，对对外开放数据进行开放前、开放中、开放后的安全管理。	1.建立数据开放发布管理制度，对对外开放数据进行开放前、开放中、开放后的安全管理和风险识别。	/
	技术保护措施	/	1.对有条件开放的数据要采取身份鉴别、使用场景识别等技术措施，确保数据不超范围使用。	1.采用隐私计算技术提供可用不可见的数据开放服务。	

参 考 文 献

[1]《政务信息资源共享管理暂行办法》（国发〔2016〕51号）
[2] GB/T 21063.4-2007 政务信息资源目录体系 第4部分：政务信息资源分类
[3] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型