

DB3202

无 锡 市 地 方 标 准

DB 3202/T 1049—2023

无锡市公共数据分类分级实施指南

2023 – 05 – 15 发布

2023 – 05 – 21 实施

无锡市市场监督管理局

发 布

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。

本文件由无锡市大数据管理局提出并归口。

本文件起草单位：无锡市大数据管理局、无锡市城市运行管理中心、北京启明星辰信息安全技术有限公司、无锡市智慧城市建设发展有限公司、无锡智发启星安全技术有限公司。

本文件主要起草人：权辉、颜春水、章瑜桢、寿孝波、郑霄、杜巍、肖梦娜、蒋子海、王娟、宋建华、刘苏涵、陈昱宁、季鹏、张维、姚方聃、刘东华、司文。

引 言

为推进公共数据共享开放，针对不同类型公共数据制定分类分级管理依据，实现公共数据价值的最大化挖掘，特制定本文件。

本文件是无锡市政府开展公共数据分类分级的顶层标准，用于指导行政机关以及履行公共管理和公共服务职能的企业、事业单位和社会组织在共享开放数据时，对数据进行分类分级提供参考，在释放公共数据资源价值的同时，不会影响到国家安全、社会秩序和公共利益。

无锡市公共数据分类分级实施指南

1 范围

本文件规定了无锡市公共数据分类分级的管理要求和流程。

本文件适用于无锡市公共数据的分类分级管理。公共管理和服务机构使用相关企业、第三方平台等数据的分类分级管理可参考执行。

本文件不适用于涉及国家秘密的公共数据管理。

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 信息安全技术 术语
- GB/T 35273 信息安全技术 个人信息安全规范
- GB/T 35274 信息安全技术 大数据服务安全能力要求
- GB/T 35295 信息技术 大数据 术语
- GB/T 37964 信息安全技术 个人信息去标识化指南
- GB/T 38667 信息技术 大数据 数据分类指南

3 术语和定义

GB/T 25069、GB/T 35273、GB/T 35274、GB/T 35295、GB/T 37964和GB/T 38667界定的以及下列术语与定义适用于本文件。

3.1

公共管理和服务机构 public management and service agencies

本市各级行政机关以及履行公共管理和服务职能的企业、事业单位和社会组织。

3.2

公共数据 public data

公共管理和服务机构在依法履行职责的过程中采集和产生的数据。

3.3

公共数据分类 public data classification

根据公共数据的属性或特征，按照一定的原则和方法对公共数据进行区分和归类，建立有条理的分类体系和排序体系，以便更好地管理和使用公共数据。

3.4

公共数据分级 public data grading

若公共数据管理活动过程的安全性遭到破坏，对行政机关、事业单位、企业、其他组织、自然人等可能产生的潜在影响，进行公共数据分级。

3.5

公共数据共享 public data sharing

公共管理和服务机构因履行职责需要，无偿使用其他公共管理和服务机构采集和产生的公共数据，或者为其他公共管理和服务机构提供公共数据的行为。

3.6

公共数据开放 public data opening

公共管理和服务机构面向公民、法人和其他组织提供公共数据供其开发利用的公共服务。

4 分类管理

4.1 分类原则

分类依据以下原则：

- a) 标准性：数据分类的指标和参数的具体实施参照国内和国外的相关标准及理论模型来执行；
- b) 稳定性：数据分类按照公共数据的特性进行科学性划分，选择公共数据相对稳定的本质属性或规则特征作为分类的基础和依据，使分类中大类的设置能覆盖公共数据各领域及相关知识范畴，能正确反映类目间的概念逻辑关系保证数据类型的稳定性；
- c) 可扩展性：数据随着信息的发展会产生相应变化及变更或者类目的增多，在进行分类时，保证类目的可扩展性，在新的类目增加时，不打乱原有的排布方式；
- d) 实用性：公共数据分类时既要体现数据资源特点，又要考虑用户的现实需求，根据具体情况使类目的设置实用和可操作。

4.2 分类维度

4.2.1 资源属性维度

按资源属性将数据分为基础信息资源、主题信息资源、部门信息资源等三种一级分类类型。基于一级分类可以对数据进行二次分类，二级子类如下：

- a) 基础信息资源分类，参考 DB32/T 4040.1-2021 中的信息资源分类，分为：综合人口、综合法人、社会信用、电子证照、自然资源和空间地理、公共等类别；
- b) 主题信息资源分类，参考 GB/T 21063.4-2007 将公共数据按照所涉及的主题进行分类。如果分类不满足工作需要，可另行根据实际业务情况建立主题；
- c) 部门信息资源分类，依据公共数据的来源部门进行分类，为履行公共管理和服务职能，依法履行职责采集和产生的信息资源的行政机关、事业单位、企业和社会组织。

4.2.2 共享属性维度

依据《无锡市公共数据管理办法》（政府令第171号）公共数据共享属性，将数据分为无条件共享、有条件共享、不予共享三类（共享属性与数据分级对应参考原则见附录A）。

4.2.3 开放属性维度

依据《无锡市公共数据管理办法》（政府令第171号）公共数据开放属性，将数据分为无条件开放、有条件开放、不予开放三类（开放属性与数据分级对应参考原则见附录A）。

4.3 分类方法

公共数据分类相关方法参照GB/T 38667的要求进行分类。

5 分级管理

5.1 分级原则

数据分级依据以下原则：

- a) 合法合规：满足国家法律法规及地方、行业相关标准规定；
- b) 可执行性：避免定级过程过于复杂，确保定级过程的可行性；
- c) 客观科学：数据定级规则满足客观性及可校验性，保证根据数据的分级规则可以判定数据的级别，并且数据的定级可审核以及复验。

5.2 分级方法

5.2.1 分级对象

数据的分级对象主要包括结构化数据和非结构化数据，数据分级的最小单元为数据项，对数据项进行分级时，默认数据项集合的安全级别为其所包含数据项级别的最高级别。非结构化数据按照其结构化标签进行分级。

5.2.2 分级规则

本文件根据公共数据管理活动中若数据发生泄露、篡改、丢失、破坏或滥用后对影响对象的影响程度及影响范围，将数据分为一级、二级、三级、四级，见表1。

表1 分级表

数据等级	定义	相关描述
一级	非敏感级	数据发生泄露、篡改、丢失、破坏或滥用后，对于行政机关、事业单位、企业、其他组织、自然人等的影响程度和影响范围符合以下条件之一： a) 对自然人不会造成隐私泄露、人身伤害、财产损失、精神损失及名誉损失； b) 不涉及商业秘密或不会影响行政机关、事业单位、企业和其他组织的运作，不损害其利益； c) 不会干扰社会秩序和损害公共利益。
二级	低敏感级	数据发生泄露、篡改、丢失、破坏或滥用后，对于行政机关、事业单位、企业、其他组织、自然人等的影响程度和影响范围符合以下条件之一： a) 对自然人造成轻微隐私泄露、人身伤害、财产损失、精神损失及名誉损失； b) 轻微涉及商业秘密或轻微影响行政机关、事业单位、企业和其他组织的运作和利益； c) 有限干扰社会秩序和损害公共利益。

表1 分级表（续）

数据等级	定义	相关描述
三级	敏感级	数据发生泄露、篡改、丢失、破坏或滥用后，对于行政机关、事业单位、企业、其他组织、自然人等的影响程度和影响范围符合以下条件之一： a) 对自然人造成较为严重隐私泄露、人身伤害、财产损失、精神损失及名誉损失； b) 较为严重涉及商业秘密或较为严重影响行政机关、事业单位、企业和其他组织的运作和利益； c) 较为严重干扰社会秩序和损害公共利益。
四级	极敏感级	数据发生泄露、篡改、丢失、破坏或滥用后，对于行政机关、事业单位、企业、其他组织、自然人等的影响程度和影响范围符合以下条件之一： a) 对自然人造成严重隐私泄露、人身伤害、财产损失、精神损失及名誉损失； b) 严重涉及商业秘密或严重影响行政机关、事业单位、企业和其他组织的运作和利益； c) 严重干扰社会秩序和损害公共利益。

5.3 数据分级安全管控要求

数据分级安全管控要求见附录B。

6 分类分级流程

6.1 流程图

数据分类分级流程见图1。

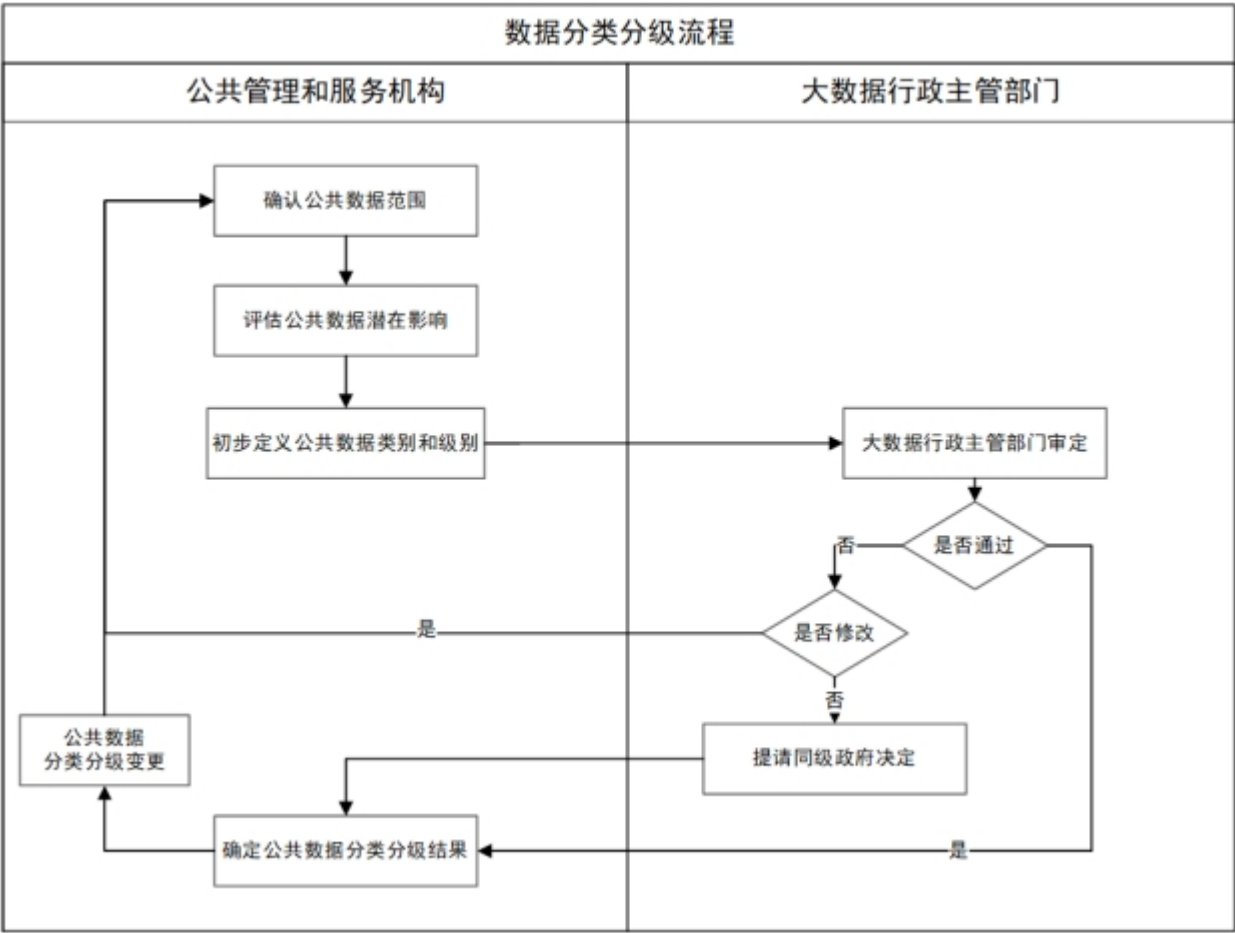


图1 分类分级流程

6.2 分类分级流程说明

6.2.1 确认公共数据范围

公共管理和服务机构在进行数据分类分级前，首先需要梳理公共数据范围及数据项清单，明确公共数据的持有者、使用者以及其他相关方，明确公共数据发生泄露后涉及到的影响对象。

6.2.2 评估公共数据潜在影响

公共管理和服务机构根据公共数据的安全性遭到破坏对影响对象产生的影响程度（无影响、轻微影响、较为严重影响、严重影响）和影响范围（较小范围和较大范围），评估公共数据潜在影响。在评估潜在影响时也可参考公共数据的共享开放属性。

6.2.3 初步定义公共数据类别和级别

公共管理和服务机构按照国家、省、市现行相关法律法规、规章制度及行业相关政策，根据本文件分类分级规则，广泛征求系统内部意见，科学论证、预测、分析，初步定义公共数据分类类别和分级级别，形成本部门公共数据分类分级结果。

6.2.4 大数据行政主管部门审定

公共管理和服务机构将本部门数据分类分级结果提交至大数据行政主管部门进行审定。大数据行政主管部门根据实际情况会同有关部门，审定公共数据分类分级结果。如不通过，双方协商重新分类分级，协商如有异议，大数据行政主管部门可提请同级政府决定。

6.2.5 确定公共数据分类分级结果

大数据行政主管部门根据审核结果，确定数据类别和级别，形成公共数据分类分级结果。

6.2.6 公共数据分类分级变更

根据数据应用场景变化及时对公共数据进行分类分级评估。当数据对象分类类别、分级级别发生变化后，在10个工作日内按照本文件重新对公共数据进行分类分级。

附 录 A
(资料性)

数据分级与共享开放对应参考原则

根据《无锡市公共数据管理办法》（政府令第171号）要求，公共数据以共享为原则，不共享为例外，数据共享对象为公共管理和服务机构，数据开放的对象为公民、法人以及其他组织等。数据共享及开放属性与数据分级的对应参考原则见表A. 1。

表A. 1 数据分级与共享开放对应参考原则

数据分级	共享	开放
一级	无条件共享	无条件开放
二级	无条件共享/有条件共享	有条件开放
三级	有条件共享	有条件开放/不予开放
四级	有条件共享/不予共享	不予开放

附 录 B
(资料性)
数据分级安全管控要求

数据分级安全管控要求见表B. 1。

表B. 1 数据分级安全管控要求

公共 数据 管理 活动	数据分级安全管控要求			
	一级	二级	三级	四级
采集	a) 应明确数据采集源、采集范围、采集方式、采集周期和频率，确保数据采集的合法性、必要性、正当性； b) 应当按照一数一源、一源多用的要求，可以通过数据共享获取的，不得重复采集、多头采集； c) 应保证采集数据的可追溯性，对数据采集全过程进行有效日志记录。	a) 应明确数据采集源、采集范围、采集方式、采集周期和频率，确保数据采集的合法性、必要性、正当性； b) 应当按照一数一源、一源多用的要求，可以通过数据共享获取的，不得重复采集、多头采集； c) 应保证采集数据的可追溯性，对数据采集全过程进行有效日志记录； d) 应采取技术手段和管理措施，防止数据采集过程中敏感数据和重要数据的泄露、篡改、丢失； e) 采集个人敏感信息时，应征得个人信息主体或其监护人的同意，应确保获得的同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示； f) 利用信息系统、网站或 APP 采集个人信息时，应依据最小化原则实现采集账号认证及权限分配，应制定隐私政策等方式明确采集个人信息的目的、类型、安全保护措施等内容，并向个人信息主体提供撤回收集、使用其个人信息的授权同意的的方法。	a) 应明确数据采集源、采集范围、采集方式、采集周期和频率，确保数据采集的合法性、必要性、正当性； b) 应当按照一数一源、一源多用的要求，可以通过数据共享获取的，不得重复采集、多头采集； c) 应保证采集数据的可追溯性，对数据采集全过程进行有效日志记录； d) 应采取技术手段和管理措施，防止数据采集过程中敏感数据和重要数据的泄露、篡改、丢失； e) 采集个人敏感信息时，应征得个人信息主体或其监护人的同意，应确保获得的同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示； f) 利用信息系统、网站或 APP 采集个人信息时，应依据最小化原则实现采集账号认证及权限分配，应制定隐私政策等方式明确采集个人信息的目的、类型、安全保护措施等内容，并向个人信息主体提供撤回收集、使用其个人信息的授权同意的的方法。	a) 经采集部门主管领导审核确认，并对授权过程进行有效记录； b) 应明确数据采集源、采集范围、采集方式、采集周期和频率，确保数据采集的合法性、必要性、正当性； c) 应当按照一数一源、一源多用的要求，可以通过数据共享获取的，不得重复采集、多头采集。采集时采用可信传输通道及经过认证的存储介质进行数据采集； d) 应保证采集数据的可追溯性，对数据采集全过程进行有效日志记录； e) 应采取技术手段和管理措施，防止数据采集过程中敏感数据和重要数据的泄露、篡改、丢失； f) 采集个人敏感信息时，应征得个人信息主体或其监护人的同意，应确保获得的同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示； g) 利用信息系统、网站或 APP 采集个人信息时，应依据最小化原则实现采集账号认证及权限分配，应通过制定隐私政策等方式明确采集个人信息的目的、类型、安全保护措施等内容，并向个人信息主体提供撤回收集、使用其个人信息的授权同意的的方法。

表B.1 数据分级安全管控要求（续）

公共数据管理活动	数据分级安全管控要求			
	一级	二级	三级	四级
传输	a) 应建立数据传输审批机制和操作流程； b) 应在网络边界做好访问控制措施； c) 应保障数据传输过程的完整性。	a) 应建立数据传输审批机制和操作流程； b) 应在网络边界做好访问控制措施； c) 应保障数据传输过程的完整性； d) 应建立安全的数据传输通道，确保数据保密性。	a) 应建立数据传输审批机制和操作流程； b) 应在网络边界做好访问控制措施； c) 应保障数据传输过程的完整性； d) 应对数据加密传输，且使用国密算法，确保数据保密性。	a) 应建立数据传输审批机制和操作流程； b) 应在网络边界做好访问控制措施； c) 应保障数据传输过程的完整性； d) 应对数据加密传输，且使用国密算法，确保数据保密性； e) 应使用数据溯源（如水印溯源）等技术，对数据泄露风险及行为进行追踪，如定位到责任人等。
存储	a) 应对存储系统的账号权限进行管理； b) 应建立数据备份机制，定期进行数据备份。	a) 应对存储系统的账号权限进行管理； b) 应建立异地数据备份机制，定期进行数据备份； c) 存储设备应采用硬件冗余保障高可用性； d) 应对存储系统的运行和访问日志进行记录、审计。	a) 应对存储系统的账号权限进行管理； b) 应建立异地数据备份机制，定期进行数据备份； c) 存储设备应采用硬件冗余保障高可用性； d) 应对存储系统的运行和访问日志进行记录、审计； e) 应采用加密机制对数据加密存储。	a) 应对存储系统的账号权限进行管理； b) 应建立异地数据备份机制，定期进行数据备份； c) 存储设备应采用硬件冗余保障高可用性； d) 应对存储系统的运行和访问日志进行记录、审计； e) 应采用国密算法加密机制对数据加密存储。
处理	a) 设置身份标识与鉴别机制； b) 应对数据操作处理行为进行记录、审计； c) 应建立数据处理过程的安全管理规章、制度和流程。	a) 应设置身份标识与鉴别机制； b) 应对数据操作处理行为进行记录、审计； c) 应建立数据处理过程的安全管理规章、制度和流程； d) 应采用去标识化技术对数据进行脱敏后供数据处理人员处理； e) 应建立数据分析结果输出的安全审查、合规风险评估和数据使用授权机制。	a) 应设置身份标识与鉴别机制，应采用双因子认证的方式对访问用户进行识别； b) 应对数据操作处理行为进行记录、审计，审计日志保存期限不低于6个月； c) 应建立数据处理过程的安全管理规章、制度和流程； d) 应采用去标识化技术对数据进行脱敏后供数据处理人员处理； e) 应建立数据分析结果输出的安全审查、合规风险评估和数据使用授权机制。	a) 应设置身份标识与鉴别机制，应采用双因子认证的方式对访问用户进行识别； b) 应对数据操作处理行为进行记录、审计，审计日志保存期限不低于6个月； c) 应建立完善的数据处理过程的安全管理规章、制度和流程； d) 应采用去标识化技术对数据进行脱敏后供数据处理人员处理； e) 应建立数据分析结果输出的安全审查、合规风险评估和数据使用授权机制。

表B.1 数据分级安全管控要求（续）

公共数据管理活动	数据分级安全管控要求			
	一级	二级	三级	四级
共享	a) 无条件对所有公共管理和服务机构数据共享。	a) 在数据共享时应严格进行审批和授权； b) 在以接口的方式共享时，需要进行接口验证及安全保护； c) 应制定数据导出的审批流程。	a) 在数据共享时应严格进行审批和授权； b) 在以接口的方式共享时，需要进行接口验证及安全保护，并对接口进行日志记录和审计； c) 应制定数据导出的审批流程。	a) 一般情况不允许共享和数据导出； b) 若需共享，应严格进行审批和授权，脱敏降级后共享。
开放	a) 无条件对所有公民、法人和其他组织进行数据开放。	a) 禁止原始数据直接开放，但是在满足审批条件，并对数据脱敏之后进行有条件开放。	a) 禁止原始数据直接开放，但是在满足审批条件，并对数据脱敏之后进行有条件开放。	a) 禁止开放。
销毁	a) 建立数据销毁审批机制，并对数据销毁过程进行记录。	a) 建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程，并对数据销毁过程进行记录； b) 应采用覆写法等方式销毁数据。	a) 建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程，并对数据销毁过程进行记录； b) 应以不可逆方式销毁数据； c) 可使用国家权威机构认证的设备对存储介质进行销毁，或联系专业机构执行销毁工作。	a) 建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程，并对数据销毁过程进行记录； b) 应以不可逆方式销毁数据； c) 宜使用国家权威机构认证的设备对存储介质进行销毁，或联系专业机构执行销毁工作。