关于印发《无锡市公共数据分类分级实施指南（试行）》的通知

各市（县）区工业和信息化局（大数据管理局）、梁溪区大数据管理局、无锡经开区经发局，市各有关单位：

现将《无锡市公共数据分类分级实施指南（试行）》印发给你们，请结合工作实际认真组织实施。

附件：无锡市公共数据分类分级实施指南（试行）

无锡市公共数据分类分级实施指南
（试行）

无锡市大数据管理局

2021 年 5 月

目录

1. 范围

根据国家相关数据安全要求、《无锡市公共数据管理办法》（政府令第171号）和《无锡市公共数据共享开放风险评估办法》（锡数发〔2020〕18号）相关要求，对无锡市公共数据实施分类分级。

本指南定义及规范了无锡市公共数据分类原则、分类方法、分级原则、分级方法、分级流程、分级安全管控等基本要求，为无锡市公共管理服务机构在公共数据分类分级中提供实施指南。

涉及国家秘密的公共数据，不在本指南的实施范围内。

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 25069　信息安全技术术语

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 37964-2019 信息安全技术 个人信息去标识化指南

GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

GB/T 36073-2018 数据管理能力成熟度评估模型

GB/T 37973-2019 信息安全技术 大数据安全管理指南

无锡市公共数据管理办法（政府令第171号）

无锡市公共数据共享开放风险评估办法（锡数发〔2020〕18号）

3. 术语、定义

3.1. 公共管理服务机构

指无锡市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

指公共管理服务机构在依法履行职责的过程中采集和产生的各类数据资源，包括结构化数据和非结构化数据，最小数据单位为数据项。

3.3. 数据分类

指根据数据的属性或特征，把具有某种共同属性和特征的数据归并到一起，并按照一定的原则和方法进行区分和归类，建立有条理的分类体系和排序体系，以便更好的管理和使用数据。

3.4. 数据分级

指若公共数据管理活动的一个或多个过程的安全性遭到破坏，按照对自然人、企业组织和事业单位以及行政机关等可能产生的潜在影响，进行数据分级。

3.5. 数据共享

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

3.6. 数据开放

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

3.7. 敏感数据

指泄漏后可能会影响国家利益、组织群体或个人带来严重危害的数据。包括个人敏感数据、企业或社会机构不适合公布的数据等。

注：个人敏感数据：身份证号码、住址、电话、银行账号、邮箱、密码、医疗信息、教育背景等；

企业或社会机构不适合公布的数据：如企业的经营情况、企业的网络结构、IP地址列表等。

3.8. 个人信息

指以电子或其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

4. 实施主体及职责

市大数据行政主管部门负责指导和监督全市公共数据分类分级工作。

其他公共管理服务机构依据本指南对公共数据进行自主分类分级。

5. 分类管理

数据分类主要为了使公共数据的管理更加有序，基于业务的分类可以更加有效的利用数据，持续性为公共管理服务机构提供精准的数据服务。

5.1. 分类原则

1) 标准性

数据分类的指标和参数的具体实施应严格依据国内和国外的相关标准及理论模型来执行。

2) 稳定性

数据分类按照公共数据的特性进行科学性划分，应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。

3) 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，应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。

4) 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，应根据具体情况使类目的设置实用和可操作。

5.2. 分类方法

按照公共数据的资源属性、共享属性、开放属性三个维度进行分类。公共管理服务机构可以参考不同的维度进行自主分类。

5.2.1. 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类型。

基础信息资源是对基础信息的分类，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。

主题信息资源按照经济社会发展的同一主题领域分为公共服务、健康保障、社会保障、食品药品安全、安全生产、价格监管、能源安全、信用体系、城乡建设、社区治理、生态环保、应急维稳、其他类型等信息资源。

部门信息资源是依据公共数据来源部门进行的分类，包括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在依法履行职责的过程中采集和产生的信息资源。

5.2.2. 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（共享属性与数据安全等级对应参考原则见 附录A数据等级与共享开放对应参考原则）。

5.2.3. 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（开放属性与数据安全等级对应参考原则见 附录A数据等级与共享开放对应参考原则）。

6. 分级管理

6.1. 分级原则

数据分级依据以下原则：

1) 合法合规

满足国家法律及地方相关标准规定。

2) 可执行性

避免定级过程过于复杂，确保定级过程的可行性。

3) 客观科学

数据定级规则应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。

6.2. 分级方法

6.2.1. 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。非结构化数据应按照其标签索引进行分级。

6.2.2. 分级规则

本指南根据公共数据管理活动中数据发生泄漏、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。

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： 1） 对自然人不会造成人身伤害、财产损失、精神损失及名誉损失； 2） 不会影响行政机关、事业单位、企业以及其他组织运作，不损害其利益； 3） 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： 1） 可能对自然人造成轻微人身伤害、财产损失、精神损失及名誉损失； 2） 有限影响一个或多个行政机关、事业单位或者严重一个或多个企业、其他组织的运作，但可以通过补救降低损失，有限影响企业和其他组织利益； 3） 有限干扰社会秩序和损害公共利益。
三级	敏感级	数据发生泄露、篡改、丢失或滥用后，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： 1） 容易对自然人造成较为严重精神损失、名誉损失、财产安全和人身伤害，但是可通过采取措施降低损失； 2） 严重影响行政机关、事业单位企业、其他组织的运作，且结果不可逆，但是可通过采取措施降低损失，工作仍可继续运转； 3） 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： 1） 危害自然人人身安全、重大财产安全； 2） 特别严重影响一个或多个行政机关、公共管理服务机构、法人和其他组织，导致工作运转失灵或几近瘫痪，或者所辖关键信息基础设施破坏严重； 3） 特别严重干扰社会秩序、严重损害公共利益。

6.3. 分级流程

数据分级流程如下图所示：

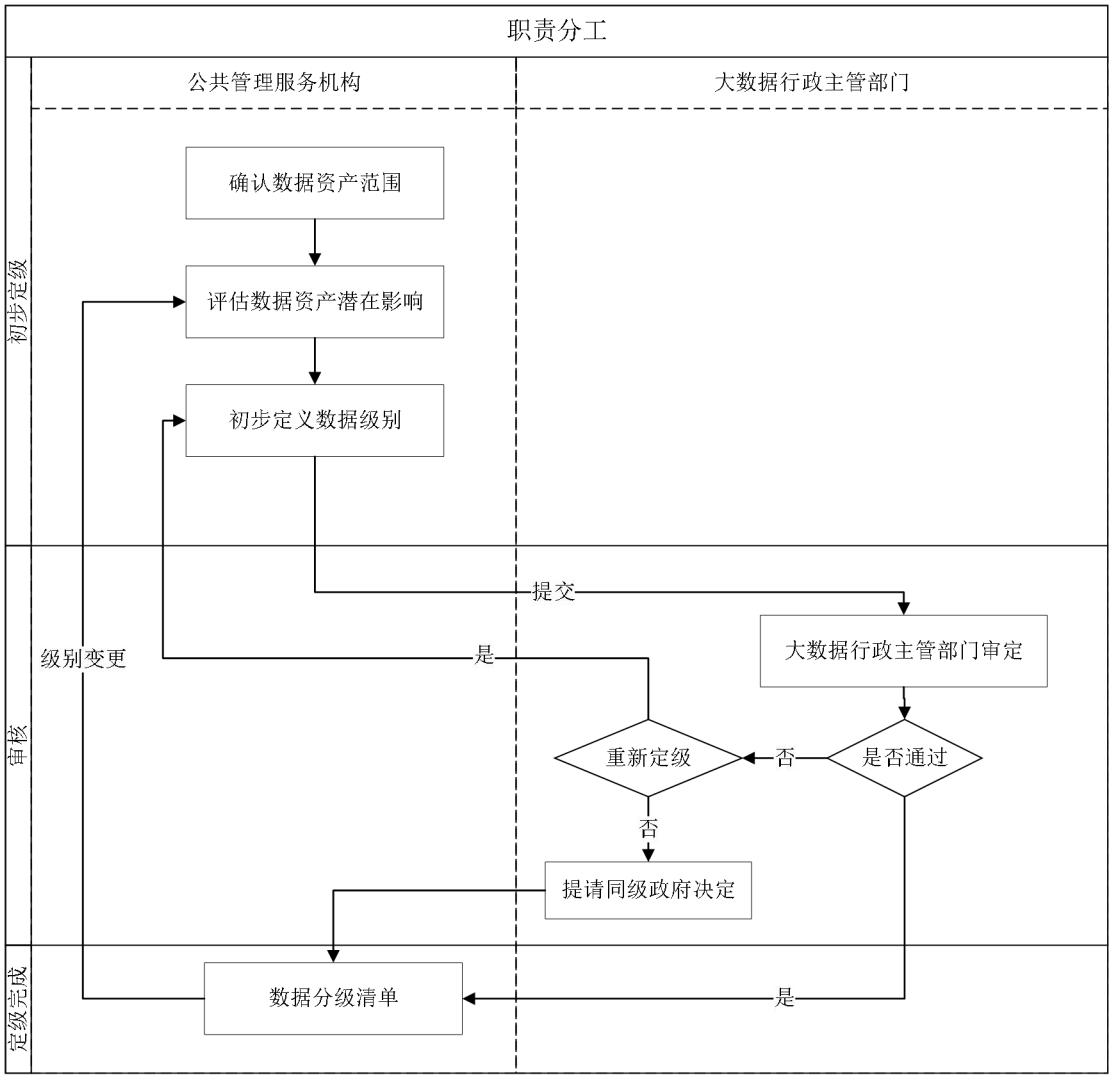

图 1 分级流程

1) 确认数据资产范围

公共管理服务机构在进行数据分级前，首先需要梳理数据资产范围及资产清单，明确数据的资产内容、资产类型、所属分类，明确数据资产的所有者、使用者以及其他相关方，明确数据发生泄露后涉及到的影响对象。

2) 评估数据资产潜在影响

公共管理服务机构应根据若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、严重影响、特别严重影响）和影响范围（较小范围和较大范围），评估数据资产潜在影响。

3) 初步定义数据级别

公共管理服务机构对照国家、省、市现行相关法律法规、规章制度及行业相关政策，根据本指南分级规则，广泛征求系统内部意见，科学论证、预测、分析，初步定义公共数据安全级别。

4) 大数据行政主管部门审定

公共管理服务机构将数据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，通过委托第三方服务等形式，以公告公示、问卷调查、座谈会、论证会等多种形式，征求意见、科学论证，审定数据安全级别。如不通过，协商确认是否重新定级，公共管理服务机构若无异议将进行重新定级，如有异议，大数据行政主管部门可提请同级政府决定。

5) 最终确定数据级别

大数据行政主管部门审核通过后，确定数据分级级别，形成数据分级清单。

6) 数据等级变更

当数据应用场景、分级对象、数据级别等方面发生变化，导致数据发生泄露、篡改、丢失或滥用后对影响对象的影响程度、影响范围发生较大变化时，应按照本指南重新对数据定级。

6.4. 数据分级安全管控要求

为更好保护数据安全，本指南依据分级结果制定数据分级安全管控要求（具体内容见附录B 数据分级安全管控要求）。

公共管理服务机构在进行数据分级安全管控时，除满足国家信息安全相关规范之外，还应满足本指南要求。

附录 A 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如下：

表 2 数据分级及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	有条件开放
	无条件共享	不予开放
	有条件共享	有条件开放
三级	有条件共享	不予开放
四级	不予共享	不予开放

附录 B 数据分级安全管控要求

表 3 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	1.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。 2.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。 3.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。	1.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。 2.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。 3.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。 4.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。 5.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。 6.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	1.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。 2.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。 3.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。 4.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。 5.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。 6.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	1.应经过主管领导审核确认进行数据采集，并对审核过程进行有效记录，确保数据采集的合法性、必要性、正当性。 2.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。 3.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。 4.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。 5.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。 6.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，必要时加入授权审批流程，应通过制定隐私

		收集、使用其个人信息的授权同意的方法。	收集、使用其个人信息的授权同意的方法。	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方法。
汇聚	1.应对存储系统账号进行统一权限管控。 2.建立数据备份机制，定期进行数据备份。 3.分析、加工数据时，应明确数据加工、分析的目标和范围，确保加工前后数据映射关系，并对输出结果建立安全审查，合规风险评估及授权机制。 4.应对数据加工、分析等处理环节的操作行为进行审计。	1.应对存储系统账号进行统一管理，通过访问控制设备进行统一授权和登录，审计登录及操作过程。 2.建立数据备份机制，定期进行数据备份。 3.分析、加工数据时，需通过审批授权，进行应用认证和授权处理的方式访问数据，数据申请时明确数据加工、分析的目标和范围，确保加工前后数据映射关系。 4.数据分析前应进行脱敏，应对数据脱敏、加工、分析等处理环节的操作进行审计，审计日志保存期限应不少于6个月。 5.原则上不允许导出数据到终端，如因业务需要，需在访问控制设备上通过二次审批，分析完成后终端上不允许保留导出的原始数据。 6.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。 7.禁止以远程方式加工和分析数据。 8.使用终端DLP设备对终端进行敏感数据	1.应对存储系统账号进行统一管理，通过访问控制设备进行统一授权和登录，审计登录及操作过程。 2.应以加密或脱敏的方式存储。建立数据备份机制，定期进行数据备份，并建立异地备份措施进行异地备份。 3.分析、加工数据时，需通过审批授权后，进行应用认证和授权处理的方式访问数据。数据申请时明确数据加工、分析的目标和范围，确保加工前后数据映射关系。 4.数据分析前应进行脱敏，应对数据脱敏、加工、分析等处理环节的操作进行审计，审计日志保存期限应不少于6个月。 5.禁止导出数据到终端。 6.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。 7.禁止以远程方式加工和分析数据。 8.使用终端DLP设备对终端进行敏感数据识别和发现，在发现终端上存在敏感数据	1.应对存储系统账号进行统一管理，通过权限管理系统进行统一授权和登录，审计登录及操作过程。 2.应以加密或脱敏的方式存储。建立数据备份机制，定期进行数据备份，并建立异地备份措施进行异地备份。 3.分析、加工数据时，需通过审批授权，进行应用认证和授权处理的方式访问数据。数据申请时明确数据加工、分析的目标和范围，确保加工前后数据映射关系。 4.数据分析前应进行脱敏，应对数据脱敏、加工、分析等处理环节的操作进行审计，审计日志保存期限应不少于6个月。 5.禁止导出数据到终端。 6.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。 7.禁止以远程方式加工和分析数据。 8.使用终端DLP设备对终端进行敏感数据识别和发现，在发现终端上存在敏感数据

		识别和发现，在发现终端上存在敏感数据时及时告知。 9.对数据汇聚通道进行加密，加密算法符合国家密码管理相关规定。	时及时告警。 9.对数据汇聚通道两端进行身份鉴别和认证，并对数据加密传输，加密算法符合国家密码管理相关规定。	时及时告警。 9.对数据汇聚通道两端进行身份鉴别和认证，并对数据加密传输，加密算法符合国家密码管理相关规定。
共享	1.无条件对所有公共管理服务机构数据共享。	1.在数据共享时应严格进行审批和授权。 2.在以接口的方式共享时，需要进行接口验证及安全保护。	1.在数据共享时应严格进行审批和授权。 2.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。	1.一般情况不允许共享。 2.若需共享，应严格进行审批和授权，脱敏降级后共享。
开放	1.无条件对所有公民、法人和其他组织进行数据开放。	1.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。	1.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。	1.禁止原始数据直接开放。

附录 C 数据分级参考示例

数据集名称：公积金个人信息表

数据项：开户日期、月缴额、职工缴存率、缴存比例、个人账号、手机号、证件号码、职工姓名、补贴个人账号。

1、数据集分析：

按照数据集分析该过程，公积金信息按照类别属于个人就业信息，影响对象为自然人，在所有数据一起被获取时，可以关联分析出其他个人敏感数据。发生泄漏、篡改、丢失、破坏或滥用后可能会对自然人造成较为严重精神损失及名誉损失以及财产安全和人身伤害，因此得出该数据集最高级别可定位为三级。

2、数据项分析：

“开户日期”、“职工姓名”、“缴存比例”、“职工缴存率”字段信息在公共管理服务机构间共享时，通过分析挖掘，无法分析出个人财产情况，但是该数据为个人隐私数据，公开后可能会对个人产生轻微影响，因此级别定级为二级，禁止原始数据直接开放。

“手机号”字段为联系信息，当发生数据泄漏时可能会引起骚扰电话，电话诈骗等情况，该过程可能会轻微影响人身安全和财产安全并且可能会除个人之外的其他人产生影响，所以该字段的安全级别定位成二级。

“月缴额”、“个人账号”、“证件号码”、“补贴个人账号”属于敏感信息，若泄露会对财产对自然人造成较为严重精神损失及名誉损失，部分财产安全和人身伤害；所以该字段的安全级别定位成三级。

表 4 数据项分级示例

数据集	数据项	影响程度	数据等级
公积金个人信息表	开户日期	轻微影响	二级
	月缴额	严重影响	三级
	职工缴存率	轻微影响	二级
	缴存比率	轻微影响	二级
	个人账号	严重影响	三级
	手机号	轻微影响	二级
	证件号码	严重影响	三级
	职工姓名	轻微影响	二级
	补贴个人账号	严重影响	三级