ICS 35.020
CCS L 60

DB36

江　西　省　地　方　标　准

DB36/T 1713—2022

公共数据分类分级指南

Local guidelines for public data classification and grading

2022－12－13 发布　　2023－06－01 实施

江西省市场监督管理局　　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。

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这些专利的责任。

本文件由江西省发展和改革委员会提出并归口。

本文件起草单位：江西省信息中心、思创数码科技股份有限公司、江西省自然资源事业发展中心、江西省人事和社会保障厅、江西省工业和信息产品监督检验院、江西省财政事务中心、江西省计算机用户协会、江西省创业就业服务中心、南昌大学信息工程学院。

本文件主要起草人：杜军龙、王磊、李桑榆、肖慧华、戴志勇、郭德斌、辜雅敏、倪志鹏。

引　言

为了规范和促进江西省公共数据开放、共享、利用与安全管理，提升政府治理能力和公共服务水平，助推数字政府、数字经济高质量发展，根据《中华人民共和国数据安全法》、《江西省公共数据管理办法》等法律、法规、规章和国家有关规定，制定本文件。

本文件是对江西省公共数据进行数据分类和分级的顶层标准，用于指导各级行政机关、公共管理和服务机构在共享和开放本单位数据时，对本单位数据进行科学分类，并对分类后的公共数据定级提供参考。在维护国家安全、社会公共利益，保护公民、法人和其他组织合法权益的前提下，实现江西省公共数据高质量共享和开放。

公共数据分类分级指南

1 范围

本文件规定了江西省公共数据的分类分级原则、定义及方法以及公共数据的安全分级管控要求。

本文件适用于指导对公共数据进行分类和定级管理，以及开展公共数据采集、存储、传输、访问、处理、共享、开放、销毁等行为的安全与管理活动。

本文件不适用于涉密公共数据的分类分级管理。

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 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

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 38667-2020 信息技术 大数据 数据分类指南

JR/T 0197-2020 金融数据安全 数据安全分级指南

DB36/T 1124-2019 江西省政务信息资源目录编制规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

公共数据 Public data

本文件所称的公共数据，是指本省国家机关、事业单位，经依法授权具有管理公共事务职能的组织，以及供水、供电、供气、公共交通等提供公共服务的组织（以下统称公共管理和服务机构），在依法履行职责和提供公共服务过程中产生或者获取的数据。

3.2

公共数据分类 Public data classification

根据公共数据的属性和特征，将其按照一定的原则和方法进行区分和归类，并建立起一定的分类体系和排列顺序，以便更好的管理和使用公共数据的过程。

3.3

公共数据分级 Public data grading

依据《中华人民共和国数据安全法》，根据数据在经济社会发展中的重要程度，按照公共数据遭到篡改、破坏、泄露或者非法获取、非法利用后对国家安全、社会秩序、公共利益或者公民、组织合法权益的危害程度对公共数据进行定级，为数据全生命周期管理的安全策略制定提供支撑。

3.4

公共数据共享 Public data sharing

依据《江西省公共数据管理办法》（江西省政府令第254号）定义公共数据共享：公共管理和服务机构之间因履行职责和提供公共服务需要通过全省统一的数据共享交换平台使用或者提供公共数据的行为。

3.5

公共数据开放 Public data opening

依据《江西省公共数据管理办法》（江西省政府令第254号）定义公共数据开放：公共管理和服务机构面向社会提供具备原始性、可机器读取、可供社会化利用的数据集的公共服务。

4 公共数据分类

4.1 分类原则

4.1.1 科学性原则

应按照公共数据的多维特征及其相互间存在的逻辑关联进行科学、系统的分类。

4.1.2 稳定性原则

应选择分类对象的最稳定的本质特征和属性为依据进行分类。

4.1.3 实用性原则

应结合现实需求，符合用户对公共数据区分和归类的普遍认知。每个类目下都有公共数据，不设没有意义的类目。

4.1.4 扩展性原则

应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。

4.1.5 唯一性原则

应保证公共数据在同一分类维度下具有唯一性，不同细分分类之间不出现交叉或者重复。

注：公共数据分类应遵循国家、地方、部门法律法规、相关规定的要求，参考GB/T 38667-2020相关国家数据分类标准对公共数据进行分类。

4.2 分类方法

4.2.1 主题分类维度

参照DB36/T 1124-2019《江西省政务信息资源目录编制规范》，对围绕经济社会发展的同一主题领域的公共数据进行分类，包括但不限于：健康保障、人力资源社会保障、食品药品安全、安全生产、价格监管、能源安全保障、城乡建设、社区治理、生态环保、应急维稳、住房保障、金融监管、信用体系建设、行政执法监督、民主法治建设、执政能力建设、投资审批、社会经济发展等。

4.2.2 部门分类维度

根据公共数据所属于（或提供公共数据）的不同组织机构进行分类，以省级部门、设区市政府为部门分类一级指标，市级部门、设区市所辖县区政府作为二级指标对公共数据进行分类，各部门按照本部门职能对数据进行细分。部门分类示例可参见附录A。

4.2.3 行业分类维度

参考GB/T 4754-2017 国民经济行业分类，根据公共数据所涉及的行业领域进行分类，包括但不限于：农、林、牧、渔业；采矿业；制造业；电力、热力、燃气及水生产和供应业；建筑业；批发和零售业；交通运输、仓储和邮政业；住宿和餐饮业；信息传输、软件和信息技术服务业；金融业；房地产业；租赁和商务服务业；科学研究和技术服务业；水利、环境和公共设施管理业；居民服务、修理和其他服务业；教育；卫生和社会工作；文化、体育和娱乐业；公共管理、社会保障和社会组织；国际组织等。行业分类示例可参见附录A。

注：本文件采用多维度和线分类法相结合的方法，在主题、部门和行业三个维度对数据项集合进行整体分类，业务部门可以对每个维度采用线分类法将其分为大类、中类和小类三级以及根据业务需要对数据分类进行小类之后的细分。

5 公共数据分级

5.1 分级原则

公共数据分级应遵循国家、地方、部门法律法规、相关规定的要求，参考GB/T 22240-2020、JR/T 0197-2020等国家、行业有关数据安全定级标准对公共数据进行定级。

5.1.1 分级管控原则

通过对公共数据进行分级，推动建立基于分级的公共数据全生命周期安全防护体系，确保在安全可控的环境下，促进公共数据共享和开放。

5.1.2 综合判定原则

公共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，应充分考虑数据聚合情况、数据体量、数据时效性、数据脱敏处理等因素，保证公共数据级别的准确性、客观性。

5.1.3 弃低取高原则

针对数据项的定级，应取该数据项所有判定结果中级别的最高值；针对数据项集合的定级，应取该数据项集合中所有数据项级别的最高值。

5.2 分级对象

从数据分级的粒度上分，可以对数据项进行分级，也可以对数据项集合进行整体分级。

5.3 分级方法

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、社会秩序、公共利益或者公民、组织合法权益，并结合江西省公共数据的实际情况，根据公共数据遭到篡改、破坏、泄露或者非法获取、非法利用（表 1 中简称“数据遭到破坏”）后，可能带来的影响程度进行安全分级，影响程度判别参考依据见表 1。

——影响对象包括：国家安全，社会秩序及公共利益，政府机构、企事业单位、其他社会组织及个人合法权益；

——影响程度包括：严重、中等、轻微、几乎无。

表1 影响程度判别参考依据

程度	定义
几乎无影响	数据遭到破坏后，对影响对象几乎不造成损害或影响微弱可以忽略。
轻微影响	数据遭到破坏后，对影响对象造成轻微损害或一般损害，范围较小、程度可控且结果可以补救。 例如：对机构的相关工作产生轻微干扰，但工作仍可正常运转；对自然人造成轻微人身伤害或轻微财产损失。
中等影响	数据遭到破坏后，对影响对象造成较为严重的损害，范围较大但程度可控、结果可以补救或范围较小、结果不可逆但可采取措施降低损失。 例如：对机构的相关工作产生较大干扰，但工作仍可继续运转；对自然人造成严重人身伤害或较大财产损失。
严重影响	数据遭到破坏后，对影响对象造成严重损害，影响的范围、程度不可控且结果不可逆。 例如：对机构的相关工作产生极大干扰，导致工作运转失灵或几近瘫痪；致使自然人死亡或导致重大财产损失。

5.4 分级规则

根据公共数据遭到篡改、破坏、泄露或者非法获取、非法利用后（表 2 中简称“数据遭到破坏”）的影响对象、影响程度来确定数据的安全级别，共分为 4 级，由高至低分别为：敏感数据（L4 级）、较敏感数据（L3 级）、低敏感数据（L2 级）、不敏感数据（L1 级），详细数据级别及分级参考判断标准见表 2。

数据分级示例可参见附录 A。

表2 数据级别与判断标准

安全等级	级别标识	定义
L1 级	不敏感	数据遭到破坏后，对公共管理和服务机构及个人合法权益几乎无影响；对社会秩序、公共利益以及国家安全几乎无影响。
L2 级	低敏感	数据遭到破坏后，对公共管理和服务机构及个人合法权益造成轻微影响；对社会秩序及公共利益、国家安全几乎无影响。
L3 级	较敏感	数据遭到破坏后，对公共管理和服务机构及个人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；对国家安全几乎无影响。
L4 级	敏感	数据遭到破坏后，对公共管理和服务机构及个人合法权益造成严重影响；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。

5.5 数据级别变更

数据分级完成后，出现下列情形之一时，公共管理和服务机构宜对相关数据的级别进行变更。数据安全级别变化事宜参见附录 B：

a）数据内容发生变化，导致原有数据的分级级别不适用变化后的数据。

b）数据内容未发生变化，但因数据时效性、数据规模、数据使用场景、数据加工处理方式等发生变化，导致原定的数据级别不再适用。

c）因数据汇聚融合，导致原有数据级别不再适用汇聚融合后的数据。

d）因国家或行政主管部门要求变化，导致原定的数据级别不再适用。

e）需要对数据级别进行变更的其他情形。

5.6 数据定级与安全管控措施

公共管理和服务机构应根据数据分级情况，对数据采集与传输、数据存储、数据访问、数据处理、数据共享、数据开放和数据销毁等数据全生命周期采取差异化的安全管控措施，数据安全级别和安全管控措施见表 3。

表3 数据安全级别和安全管控措施

类别	L1 级	L2 级	L3 级	L4 级
数据采集与传输	公共数据采集设备应符合安全认证，采集流程和方式符合相应要求，对授权采集的过程和信息进行日志记录。	同 L1 级	在满足 L2 级的基础上，根据数据提供方的要求，对跨级跨域的数据采集和传输进行链路加密、敏感信息和字段的脱敏、权限的访问控制等安全措施。	在满足 L3 级的基础上，满足: 1、采用身份鉴别机制、指纹识别等，对数据采集源(人员、终端、数据库等)识别和记录。 2、建立数据质量管理机制，确保采集数据的质量。 3、应遵循《中华人民共和国密码法》的要求，使用通过国家密码管理局认证的密码技术和密码产品实现“身份鉴别”。
数据存储	1、公共数据应保存在可信或可控的信息系统、物理环境中。 2、应建立数据备份机制，定期进行数据的备份。	在满足 L1 级的基础上，对存储数据的访问进行日志记录和审计，以及对运维人员权限的分配和控制。	在满足 L2 级的基础上，满足: 1、对多租户逻辑存储需要租户隔离、授权管理规范。 2、需要采用加密技术对存储数据进行加密。	在满足 L3 级的基础上，使用通过国家密码管理局认证的密码技术和密码产品实现“防篡改”。

表 3 数据安全级别和安全管控措施（续）

类别	L1 级	L2 级	L3 级	L4 级
数据访问	可采用口令、密码、生物识别等鉴别技术对用户进行身份鉴别。	在满足 L1 级的基础上，对数据访问行为、访问内容、访问频率等访问情况进行审计、分析。	在满足 L2 级的基础上，应采用口令、密码、生物识别等两种或两种以上组合的鉴别技术对用户进行身份鉴别。	在满足 L3 级的基础上，应持续对用户账号进行风险监测，并对账号进行动态授权。
数据处理	1、设置身份标识与鉴别机制。 2、对数据的分析处理过程进行统一的日志记录。	在满足 L1 级的基础上，对运维人员进行权限的分配和控制。	在满足 L2 级的基础上，增加: 1、对分析处理的环境采取网络隔离、访问控制、身份认证等安全防护措施。 2、对源数据和分析结果的数据加密存储和防泄漏。	在满足 L3 级的基础上，增加: 1、对部分敏感信息需要进行去标识化处理。 2、对操作过程进行日志记录。
数据共享	对数据共享的过程进行日志记录。	在满足 L1 级的基础上，对运维人员进行权限的分配和控制。	在满足 L2 级的基础上： 1、视情况脱敏。 2、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。 3、对数据共享全链路各环节风险进行监控。 4、数据共享审批日志记录的审计。	不予共享
数据开放	对数据开放的过程进行日志记录。	在满足 L1 级的基础上，视情况脱敏。	在满足 L2 级的基础上： 1、脱敏后受限开放。 2、对数据开放全链路各环节的权限最小化控制，如进行白名单控制并对异常进程监控。 3、数据开放审批日志记录的审计。	不予开放
数据销毁	是否销毁依实际情况，如采取销毁手段，则需对销毁过程进行记录。	建立数据销毁和存储媒介销毁审批机制，业务终止时宜采用删除、覆写法等方式销毁有关数据，并对销毁过程进行记录。	建立数据销毁和存储媒介销毁审批机制，业务终止时应以不可逆的方式销毁有关数据，并对销毁过程进行记录。	同 L3 级

5.7 共享开放级别

公共管理和服务机构基于公共数据的敏感程度及自身业务需求定义数据的共享和开放范围，公共数据共享开放级别见表 4。

表4　公共数据共享开放级别

	对照关系			
数据安全等级	L1 级	L2 级	L3 级	L4 级
共享属性	无条件共享	有条件共享		不予共享
共享条件	各级数据资源管理部门在全省统一的数据共享交换平台审批后无条件共享。	各级数据资源管理部门和数据提供单位在全省统一的数据共享交换平台审批后有条件共享。	数据视情况进行脱敏或隐去关键信息，降低安全级别后，各级数据资源管理部门和数据提供单位在全省统一的数据共享交换平台审批；或经数据提供单位授权后，各级数据资源管理部门审批后有条件共享。	不予共享类公共数据依法经过脱密、脱敏处理降低安全级别后且相关权利人同意共享的，可以列入无条件共享类或者有条件共享类。
开放属性	无条件开放	有条件开放		不予开放
开放条件	用户在各级公共数据开放平台登录后可直接下载。	数据视情况进行脱敏或隐去关键信息，降低安全级别后，各级数据资源管理部门和数据提供单位在全省统一的数据共享交换平台审批；或经数据提供单位授权后，各级数据资源管理部门审批后有条件开放。	数据经脱敏或隐去关键信息，降低安全级别后，各级数据资源管理部门和数据提供单位在全省统一的数据共享交换平台审批；或经数据提供单位授权后，各级数据资源管理部门审批后有条件开放。	不予开放类公共数据依法经过脱密、脱敏处理降低安全级别后或者相关权利人同意开放的，可以列入无条件开放类或者有条件开放类。

附 录 A
（资料性）
公共数据分类分级示例

A.1 数据分类

示例1-数据集名称：婚姻登记信息（XX市民政局）

数据集按部门分类属于 XX 市大类，按线分类法划分中类属于 XX 市民政部门中类，按照部门职能细分属于社会事务小类。

示例 2-数据集名称：工程竣工验收信息

数据集按行业分类属于建筑业大类，按线分类法划分中类属于房屋建筑业中类。

A.2 数据分级

示例

数据集名称：婚姻登记信息

数据项：当事人婚姻登记类别、登记时间、配偶姓名、身份证件类型及号码、户籍地址、婚姻登记机关名称

数据项定级：

L1 级：登记时间，婚姻登记机关名称为低风险的数据项，如果泄露对个人权益不造成影响或影响微弱可以忽略，列入 L1 级数据。

L2 级：当事人婚姻登记类别，配偶姓名，户籍地址属于个人低敏感数据，列入 L2 级数据。

L3 级：身份证件类型及号码属于个人较敏感数据，列入 L3 级数据。

数据项集合定级：

按照数据分类的弃低取高原则，针对数据项集合的定级，应取该数据项集合中所有数据项级别的最高值，所以列入L3级数据。

附 录 B
（资料性）
数据安全级别变化事宜

导致数据发生升降级的主要技术手段有数据脱敏、数据汇聚融合、改变数据提供方式等。其中数据脱敏后产生的数据，其安全级别通常低于脱敏前的数据。而汇聚融合是指对数据进行集中、清洗、转换、重组、关联分析、多方计算等处理的过程，相对于汇聚融合前数据的安全级别，经过不同的数据汇聚融合处理手段所产生的数据，其安全级别可能上升，也可能下降。数据提供方式的不同可导致数据可见内容的变化，数据可见内容受到限制时，其安全级别可降低。

数据安全级别变化的示例，见表 B.1。

表B.1 数据安全级别变化示例表

序号	措施	安全级别调整
a	数据内容发生变化，导致原有数据的分级级别不适用变化后的数据： 从数据中去除能够直接定位到信息主体的内容，删除涉及政府敏感信息的内容等，特定时间或事件后数据失去原有敏感性	级别相应降低
b	数据内容未发生变化，但因数据时效性、数据规模、数据使用场景、数据加工处理方式等发生变化，导致原定的数据级别不再适用： 数据内容未发生变化，但数据更新频率从每日更新调整为每年更新	级别相应降低
c	因数据汇聚融合，导致原有数据级别不再适用汇聚融合后的数据： 汇聚融合，特定部门特定时间或事件后数据具有高安全等级	级别相应升高
d	因国家或行政主管部门要求变化，导致原定的数据级别不再适用： 响应国家政务数据共享工作要求，特定部门不予共享数据因特定事件需要对其他单位共享使用	级别相应降低
e	需要对数据级别进行变更的其他情形： 数据采用接口方式提供服务，且该接口本身带有用户身份鉴别功能，只供经过身份验证的本人确认授权后的操作使用	级别相应降低

参 考 文 献

[1] 《江西省数据应用条例（草案）》
[2] 《工业数据分类分级指南（试行）》
[3] 基于《数据安全法》的数据分类分级方法研究(《信息安全研究》|2021 年第 010 期|P.933-940)