ICS 35.240.01
CCS L 70

团　　体　　标　　准

T/ZSIA XXXX—2026

城市运营服务数据管理通则

General rules for data management of urban operation service

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

浙江省软件行业协会　　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专利的责任。

本文件由杭州市城市建设投资集团有限公司提出。

本文件由浙江省软件行业协会归口。

本文件起草单位：杭州市城市建设投资集团有限公司、・・・。

本文件主要起草人：

城市运营服务数据管理通则

1 范围

本文件规定了城市运营服务数据管理的数据对象、数据资源编目、数据收集、数据存储、数据治理、数据流通、数据服务、数据退役、数据安全。

本文件适用于城市水务、公共交通、能源保障、城市建设、住房管理等城市运营服务数据的管理。

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 17859 计算机信息系统 安全保护等级划分准则

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 37025 信息安全技术 物联网数据传输安全技术要求

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

GB/T 43697 数据安全技术 数据分类分级规则

CJ/T 545 城市运行管理服务平台数据标准

3 术语和定义

GB/T 35295界定的以及下列术语和定义适用于本文件。

3.1

数据治理 data governance

对数据资源管理行使权力和控制的活动集合（计划、监督和执行）。

[来源：GB/T 44109—2024，3.1]

3.2

元数据 metadata

关于数据或数据元素的数据（可能包括其数据描述），以及关于数据拥有权、存取路径、访问权和数据易变性的数据。

[来源：GB/T 5271.17—2010，17.06.05]

3.3

数据质量 data quality

在指定条件下使用时，数据的特性满足明确的和隐含的要求的程度。

[来源：GB/T 25000.24—2017，4.11]

3.4

数据标准 data standard

数据的命名、定义、结构和取值规范方面的规则和基准。

[来源：GB/T 36344—2018，2.8]

4 数据对象

4.1 数据分类

城市运营服务数据应基于业务领域、应用场景及数据属性进行分类。分类应遵循稳定性与灵活性相结合的原则，典型的数据分类领域包括（但不限于）：

a) 基础保障类： 涉及城市运行底座的支撑数据（如城市水务、能源保障、环境卫生等领域）；
b) 公共交通类： 涉及城市人员及物资流动的监测与调度数据（如轨道交通、公共汽电车、路网运行等领域）；
c) 城市建设类： 涉及城市空间规划与工程建设全生命周期数据（如规划审批、房产管理、工程监管等领域）；
d) 综合管理类： 涉及城市运营主体的行政办公、财务经营及应急指挥等支撑数据。

注：具体的业务场景可根据实际管理需求，在上述分类基础上进一步细化。

4.2 数据分级

数据根据安全级别不同可分为：
a) L1（不敏感）：通过一般公开渠道可获取的数据。
b) L2（低敏感）：内部生产经营的数据，用于一般业务使用。
c) L3（较敏感）：在 L2 级别的基础上，一旦泄露会带来直接经济损失或名誉损失的数据。
d) L4（敏感）：在 L3 级别的基础上，一旦泄露还会对社会及其他组织造成损害的数据。

5 数据管理架构

5.1 管理原则

5.1.1 在数据生存全周期内，开展数据质量管理和数据安全管理。
5.1.2 根据数据来源、数据共享限制等对数据进行分类和分级管理，数据分类和分级应符合本文件第 4 章的要求。
5.1.3 参与城市运营服务数据相关工作的组织、个人都是数据管理的主体，确保数据的客观真实。

5.2 管理架构

城市运营服务数据管理架构见图1，包括：
a) 数据生存周期管理：
   1) 数据采集；
   2) 数据存储；
   3) 数据处理；
   4) 数据共享；
   5) 数据流通；
   6) 数据退役；
b) 数据治理：
   1) 数据资源编目；
   2) 数据追溯；
c) 数据质量管理；
d) 数据安全管理。

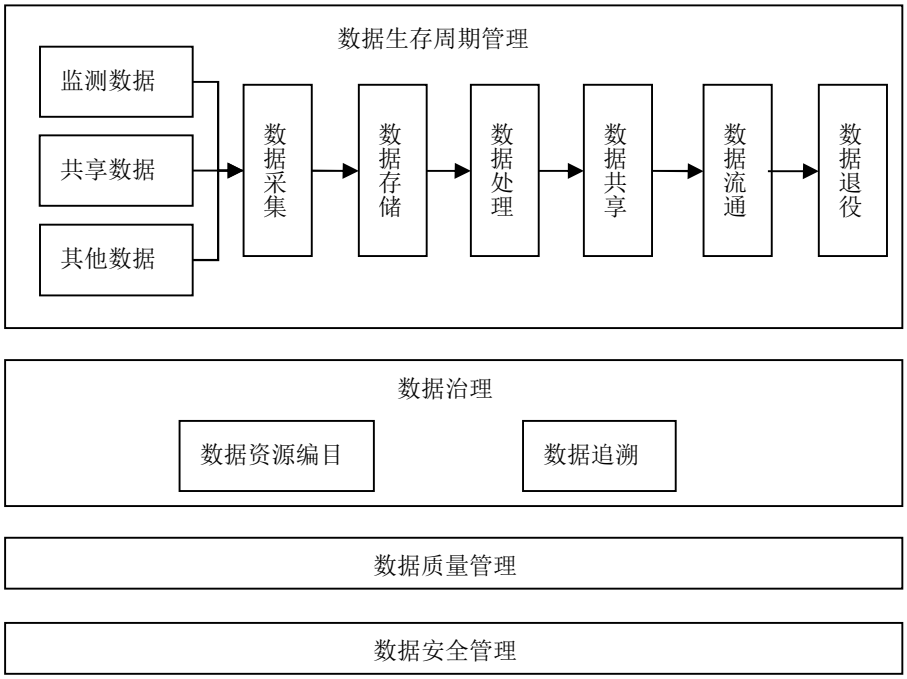

图1　城市运营服务数据管理架构

5.3　元数据管理

5.3.1　元数据管理应符合以下要求：

a）　建立元数据管理机制，明确元数据的管理过程及角色职责；
b）　明确元数据管理的范围和优先级，构建元数据库；
c）　建立完整的数据字典、数据模型、数据架构及其管理体系；
d）　建立元数据创建、维护、整合、存储、分发、查询、报告和分析机制；
e）　建立元数据管理的质量标准和评估指标，开展元数据绩效评估并持续改进。

5.3.2　元数据管理应采用三层采集架构，具体如下：

a）　技术元数据：覆盖数据库表结构、ETL 转换规则等 IT 基础设施；
b）　业务元数据：包含指标定义、业务术语等业务语义信息；
c）　管理元数据：记录数据责任人、访问权限等管控要素。

6　数据生存周期管理

6.1　数据采集

6.1.1　数据源

6.1.1.1　自动监测数据

6.1.1.1.1　主要包括自动监测站点实时监测数据，由自动采集设备进行实时采集或人工不定时监测获得。经由采集设备前端数据库传输到各相关数据负责单位或数据中心，通过共享设置可共享交换到其他使用单位。

6.1.1.1.2　对于实时监测数据应尽量避免人工干预。监测站点宜根据数据实际情况确定数据值的有效范围和预警范围，便于自动判断数据的有效性及进行数据预警。

6.1.1.2　外单位共享数据

包括上位系统的回传数据及其他单位的共享交换数据。

6.1.1.3 其他数据

其他途径获得的数据。

6.1.2 数据内容

数据采集内容应包括但不限于城市水务、公共交通、能源保障、城市建设、住房管理相关的基础数据、运营数据和服务数据。

6.1.3 数据类型

城市运营服务数据按数据结构可分为：

a) 结构化数据：电子化、规范化的数据，数据项设计、格式等均满足融合需求，无需做进一步的处理即可使用，主要包括数据库数据、电子表格数据、地理信息数据等；
b) 半结构化数据：电子化、规范化的数据，但数据项格式需进行一定处理后，才能满足数据融合的使用要求，主要包括文本、网页、日志文件、XML 文件等；
c) 非结构化数据：没有明确结构约束的数据，主要包括图片、图像、音频、视频、纸质扫描件等。

6.1.4 采集方法

城市运营服务数据接入方法包括但不限于：

a) 数据库：建立源数据库结构与目标数据库之间的存储结构映射，通过数据库同步进行采集，数据库建设符合 CJ/T 545 的要求；
b) 文件：通过文件导入进行采集，对于非结构化文件数据，可将文件整体上传至服务器后建立存储路径表；
c) API 接口：
    1) 针对结构化和半结构化文件，应建立源接口返回数据结构与目标数据库之间存储结构映射，可通过搜索进行接口数据采集，也可直接存储接口的基本信息；
    2) 针对返回非结构化接口类型，直接存储接口基本信息；
d) 消息队列：建立源数据结构与目标数据库之间存储结构映射，通过订阅消息队列进行采集。

6.1.5 采集要求

数据采集应符合的要求包括但不限于：

a) 明确采集数据目的和用途，明确采集源、采集范围、采集频率；
b) 开展全面分析，设置数据采集策略，如采集周期、采集方式、采集内容等：
    1) 业务分析，对数据来源业务进行分析；
    2) 接入方式分析，对源数据存储位置、接入方式进行分析；
    3) 结构分析，对数据的含义、类型、长度、结构进行分析；
    4) 内容分析，对数据长度、分布状态、平均值、中位数、极值等进行统计分析；
    5) 关联分析，对数据之间存在的依赖关系、主外键关系进行分析；
c) 制定采集数据的清洗、转换、加载等操作规范，做好采集数据的备份工作；
d) 对不同类别、级别的数据制定并实施不同的采集策略，做好采集过程的安全防护措施；
e) 遵循数据最小化原则，只采集满足业务所需的最少数据；
f) 制定采集数据的质量保障规则，明确数据质量保障的策略、规程和要求；
g) 对采集行为进行日志记录和安全审计。

6.2 数据存储

6.2.1 存储架构

数据存储架构应遵循分层设计原则，根据业务需求从数据源层开始，依次通过数据源层或者数据接入层（ODS）、明细层（DWD）、主题汇总层（DWS）、应用层（ADS），最终向业务应用层输出数据，具体如下：

a) 数据源层：提供原始数据，包含城市水务、公共交通、能源保障、城市建设、住房管理等业务系统数据；
b) 数据接入层（ODS）：存储外部源数据的全量或增量抽取数据，保持与源系统数据一致；
c) 明细层（DWD）：存储标准化、一致化的基础数据；
d) 主题汇总层（DWS）：按业务场景进行数据整合与轻度汇总，支持多维分析；
e) 维度层（DIM）：存储维度数据和规则，便于数据理解和分析；
f) 应用层（ADS）：面向业务需求，提供统计、分析和计算服务。

6.2.2 存储技术

数据存储技术应根据业务场景选择数据库、数据仓库、大数据平台等，具体适用范围如下：
a) 数据库：适用于事务处理系统，适合结构化数据；
b) 数据仓库：适用于历史数据存储与复杂查询，适合结构化数据；
c) 大数据平台：适用于海量数据处理与实时分析，适合多种数据类型。

6.2.3 存储格式

数据存储格式应根据业务场景选择分布式块存储、分布式文件存储和对象存储，具体要求如下：
a) 分布式块存储：支持 iSCSI/RBD 接口、多副本或纠删码冗余、卷扩容、快照、克隆、迁移等功能；
b) 分布式文件存储：支持大规模数据读写、海量文件存储、跨机房容灾、文件快照、分级存储等功能；
c) 对象存储：支持海量数据存储、文档、图片、视频、音频、日志文件等非结构化数据存储等功能。

6.2.4 存储介质

存储介质应包括云磁盘、高效磁盘、对象存储等，应能支持数据在不同介质间转移。

6.3 数据处理

6.3.1 清洗比对

数据清洗比对内容包括但不限于：
a) 残缺数据处理：确定范围、去除重要性低字段、填充缺失内容；
b) 错误数据处理：处理格式内容错误、逻辑错误、不合规等问题；
c) 重复数据处理：对重复出现的数据进行整合。

6.3.2 标签管理

以每条记录为单位进行标签处理，标签将跟随该数据记录在后续数据清洗、加工、整合等过程中流转，实现数据的溯源。标签应具有唯一性。

6.3.3 数据校验

校验结果应准确、清晰、明确、客观，并进行唯一标识。数据校验方法包括但不限于：
a) 数据可视化：通过数据可视化工具，将数据转换为图形或图表的形式，更直观地理解和分析数据；
b) 数据预处理：通过多种预处理算法对数据进行预处理，如空值插补、去重、字段过滤等；
c) 数据比较：将数据与预期结果进行比较，以确定数据是否存在问题；
d) 数据统计分析：通过数据统计分析方法，如平均值、中位数、标准差等，对数据进行描述和分析，进一步发现异常值和趋势等问题；
e) 数据建模：通过建立数据模型，对数据进行预测和分类，验证数据的准确性和有效性；
f) 数据审计：对数据的来源、传输、存储等环节进行审计，确保数据的完整性、保密性和可用性。

6.3.4 关联映射

关联映射方式包括但不限于：

a) 目标结构分析：根据源数据结构和目标结构的模型进行比对，针对字段名等进行分析比对，分析数据项映射关系，实现源字段和目标字段映射的自动匹配；
b) 事实表比对映射：根据目标结构分析和数据转换规则，实现源数据结构的类型转换、字段拆分、字段合并、字符串处理、日期转换、算术运算等数据转换；
c) 代码比对映射：根据代码数据转换规则完成源数据代码与标准代码比对映射。

6.3.5 数据整合

数据整合方式包括但不限于：

a) 水平整合：
   1) 同一实体相同维度的数据进行水平整合，数据间存在结构差异的进行统一；
   2) 对不同来源的冲突数据，能判别数据有效性、正确性则保留符合项，否则应追溯增加数据来源标识后保留。
b) 垂直整合：
   1) 对同一实体不同维度的数据进行垂直整合；
   2) 识别并提取出有效的业务主键，根据业务主键进行关联整合；
   3) 保留整合数据的来源信息；
   4) 对字段重合度低的数据，采用主从表的方式进行整合。

6.3.6 数据挖掘

数据挖掘方式包括但不限于：

a) 通过统计分析类算法对数据进行统计分析，如协方差矩阵、方差、标准差等；
b) 使用机器学习算法执行机器学习任务，如线性回归、决策树等，算法类型包括但不限于文本分析、分类、聚类、回归、推荐、关联分析等；
c) 采用大数据、人工智能等先进技术，对城市生态环境数据进行统计和分析，形成多维度的数据报表为业务决策提供支撑。

6.4 数据共享

6.4.1 共享方式

共享方式主要包括：

a) 接口共享方式：依托数据运营平台实现数据单条查询或校核比对，适用于灵活性要求较高、数据量较小的数据共享；
b) 数据共享方式：依托数据运营平台对数据进行分析计算并导出分析结果，或导出批量原始数据，适用于更新频繁、数据量较大的数据共享。

6.4.2 共享流程

6.4.2.1 共享申请

6.4.2.1.1 使用数据的机构按照“一场景一申请”的原则，应根据业务需求和使用用途提出共享申请，通过检索资源服务目录，完整、规范、准确填写对应的数据服务申请表，提交至数据运营平台，主要包括：

a) 申请接口共享的，填写共享数据服务申请表；
b) 申请流量共享的，主要包括：
   1) 对于分析计算并导出分析结果的，填写批量分析数据服务申请表；
   2) 对于导出批量原始数据的，应提供本单位数据安全管理制度，明确安全责任人和安全权责，完成数据安全防护能力自评估后，填写批量导出数据服务申请表。

6.4.2.1.2 使用数据的机构应填写公共数据规范使用承诺书，按照承诺书要求规范使用数据。

6.4.2.1.3 对于未纳入资源服务目录的数据需求，使用数据的机构应向提供数据的机构提出数据需求申请。

6.4.2.2 共享审核

6.4.2.2.1 数据工作主管部门负责开展形式审核，审核内容包括申请信息填写的完整性、规范性和准确性等。

6.4.2.2.2 提供数据的机构负责开展内容审核，按照规定的共享条件以及使用数据的机构履行职责的需要进行审核，审核内容包括申请依据充分性、数据使用范围合理性、应用场景匹配性等。

6.4.2.2.3 数据工作主管部门应对无条件共享的共享申请进行形式审核，形式审核通过后，使用数据的机构获取数据；形式审核不通过的，数据工作主管部门应依据相关法律法规说明具体理由，并反馈至使用数据的机构。

6.4.2.2.4 数据工作主管部门应对有条件共享的数据进行形式审核，形式审核通过后，提供数据的机构进行内容审核，形式审核不通过的，数据工作主管部门应依据相关法律法规说明具体理由，并反馈至使用数据的机构。

6.4.2.2.5 提供数据的机构应对通过形式审核的共享申请进行内容审核，内容审核通过后，使用数据的机构获取数据；内容审核不通过的，提供数据的机构应依据相关法律法规说明具体理由，反馈至使用数据的机构。

6.4.2.3 共享数据

6.4.2.3.1 提供数据的机构应按照申请的服务方式提供共享服务。若采用接口共享方式，数据工作主管部门、提供数据的机构应开发接口，并与使用数据的机构进行 API 接口对接；若采用数据共享方式，提供数据的机构可利用多租户、可信服务等方式提供服务。

6.4.2.3.2 提供数据的机构应按照 GB/T 43697 要求开展数据分类分级。

6.4.2.3.3 当使用数据的机构提出使用不予共享数据时，提供数据的机构应与使用数据的机构协商解决，仍未解决的应由同级数据工作主管部门协调解决。

6.4.2.4 共享应用

6.4.2.4.1 使用数据的机构应对共享的数据范围、内容等进行确认，若不符合需求应通过数据运营平台反馈。

6.4.2.4.2 使用数据的机构应按照约定方式、范围等开展数据应用，并定期将应用成效反馈至数据工作主管部门。

6.4.2.4.3 使用数据的机构在应用过程中发现的问题数据，应通过数据运营平台反馈至提供数据的机构，由提供数据的机构进行问题数据校核，提供准确数据，对无法完成校核的，应说明理由。

6.4.2.4.4 使用数据的机构应接受数据工作主管部门对应用情况的监测，监测内容包括调用类型、数量、频次、应用场景等。

6.5 数据流通

6.5.1 数据流通应依托具备安全隔离与审计追踪能力的可信数据环境开展，明确参与流通的数据提供方、加工方及使用方的权责边界。各方应依照相关数据合规流通管理办法，在严格履行审批与授权程序后规范开展数据流通活动。

6.5.2 参与跨组织数据流通的各方实体应在流通前通过主体资质与数据安全保障能力审核，建立标准化的准入评估机制，并通过签署数据安全承诺书或服务级别协议（SLA）等方式明确数据处理的责任边界，确保参与方具备与所处理数据级别相匹配的防护基础。

6.5.3 数据流转申请应严格落实“一场景一审批”原则，在明确具体业务用途、调用频次及使用有效期限的基础上，依据数据资源的安全级别与权属关系，采用动态授权机制执行最小权限管控，严禁任何超范围或超期限的数据访问。

6.5.4 跨单位数据的流转与加工应依托逻辑隔离或物理隔离的可信数据空间，应通过部署沙箱环境、隐私计算或受控容器等技术防范手段，确保核心数据的处理过程在封闭的计算域内进行，阻断非授权的外部网络直连。

6.5.5 在数据加工阶段应建立自动化的作业调度与流转机制以防范人工干预越权，严格坚守“原始数据不出域、数据可用不可见”的安全红线，系统层应具备强制屏蔽终端本地下载与截屏的能力，严禁任何形式的违规落盘、复制与明文外发。

6.5.6 任何加工形成的数据产品或服务在正式对外输出前，均应通过防泄露合规性与数据脱敏技术的双重审查，且流通全链路应自动留存包含操作主体标识、接口对接详情、数据吞吐量及时间戳的完整审计日志，保障去向与行为的全程可溯源验证。

6.6 数据退役

6.6.1 总则

数据退役应制定明确的触发条件和审批流程。对于达到留存期限或业务不再需要的数据，应执行归档或销毁操作，确保数据不再被非法访问。

6.6.2 数据归档

6.6.2.1 数据归档应满足以下要求：

a) 合规性：需依据《数据安全法》等法规明确留存期限，不得擅自缩短或延长；
b) 安全性：对含客户隐私（如身份证号）、商业机密（如合作底价）的数据需进行脱敏（如隐去身份证中间字段）或加密（采用 AES-256、SM4 等算法），防止泄露；
c) 可追溯性：全程记录归档数据来源、存储位置、访问记录，确保后续审计或业务调用时可查可证。

6.6.2.2 数据归档应按照以下方法进行：

a) 先对数据预处理，剔除重复、无效信息，统一格式（如文本转 PDF/A、结构化数据转 CSV）；
b) 按留存需求选择存储介质，长期合规数据用“磁带库+合规云”双备份（兼顾成本与安全性），短期业务数据（如活动数据）用本地高性能存储（方便调用），特殊敏感数据用物理隔离设备（避免网络风险）；
c) 执行“申请-审核-迁移-验证”流程，由归档需求人员发起申请，领导审批审核留存必要性，运维人员完成数据迁移后验证完整性，归档记录需留存至数据销毁后 1 年，到期后按对应规则（如长期数据用物理删除、短期数据用逻辑删除）处理。

6.6.3 数据销毁

6.6.3.1 数据销毁应满足以下要求：

a) 合规性原则：所有销毁操作需符合国家法律法规及行业监管要求，如《中华人民共和国个人信息保护法》中“个人信息删除后不得留存副本”的规定，确保销毁行为合法可追溯；
b) 分级分类原则：根据数据敏感级别与存储形式，选择适配的销毁方式（如核心敏感数据需物理删除，非敏感临时数据可逻辑删除），避免过度销毁或销毁不彻底；
c) 最小影响原则：销毁过程需避开业务高峰期（如财务结账日、月度报表生成时段），提前告知相关业务部门，确保不影响正常业务开展；
d) 可追溯原则：所有销毁操作需留存完整记录（申请单、审批意见、操作日志、检测报告），便于后续审计与问题追溯。

6.6.3.2 数据仓库配套存储介质达到使用年限（硬盘一般不超过 5 年）、出现物理损坏（如硬盘坏道率超 1%、存储阵列部件故障）或因系统升级需报废，且介质内存储核心敏感数据（如客户支付信息、商业合作底价、未公开财务数据）时，应执行介质销毁，禁止将未销毁的介质流转至外部或二次使用。销毁方法有以下 3 种：

a) 传统机械硬盘/存储阵列硬盘：销毁前应由运维人员从数据仓库存储集群中移除设备，注销其在系统中的设备编号（避免残留设备信息影响集群稳定性）；优先采用专业消磁设备处理，消磁强度不低于 8500 奥斯特，确保磁盘磁道信息彻底清除；消磁后需在信息安全部人员监督下进行物理粉碎，粉碎颗粒直径≤5 mm，防止通过技术手段重组磁盘恢复数据；
b) 云存储资源：若数据仓库使用云存储，需向云服务商明确要求删除底层存储块（而非仅删除数据索引），并要求服务商出具“数据零残留”证明（需包含销毁时间、存储块编号、检测结果）；同时由运维人员清理本地数据仓库与云存储的同步链路配置（如关闭数据同步任务、删除访问密钥），防止数据二次同步至云存储；

c） 特殊介质：SSD 固态硬盘（因无物理磁道，消磁无效）需采用“芯片拆解+物理粉碎”方式，先拆除固态硬盘的存储芯片，再对芯片进行粉碎处理；移动存储设备（如专用 U 盘、移动硬盘）需参照硬盘销毁标准执行消磁（可兼容的设备）或物理粉碎，禁止直接丢弃。

6.6.3.3 数据仓库中非敏感临时数据经数据仓库管理员联合数据所属业务部门确认数据无留存必要时应进行逻辑删除，且删除后不影响业务查询、历史追溯及报表生成的场景。应采用数据仓库通用工具执行删除，避免使用可能影响全表数据的命令（如仅针对指定时间分区执行删除）；删除后需通过数据查询与分析工具验证目标分区及数据已不可见，同时检查关联业务报表的数据完整性，确保无业务数据缺失或异常。

6.6.3.4 数据仓库中核心敏感数据无需继续保留，但存储介质（如数据仓库核心服务器硬盘、分区存储、云硬盘）仍需继续使用时，应进行物理删除，具体操作如下：

a） 数据隔离与合规审核：删除前需在数据仓库中对目标数据进行“软隔离”——标记为“待删除”状态并限制所有用户的查询权限，同时进行最后一次合规检查，确认数据无留存必要，出具《核心数据删除审计确认书》；若涉及客户个人信息，还需核对《中华人民共和国个人信息保护法》中“删除权”相关要求，确保删除行为符合客户意愿或法规规定；

b） 多层覆盖删除：结合数据仓库存储特性，分三层执行物理删除，确保无数据残留：

1） 第一层：使用数据仓库工具对目标数据所在的存储块进行标记；

2） 第二层：对标记的数据仓库文件，由运维人员登录目标数据节点彻底清除磁盘块中的数据，避免残留数据；

3） 第三层：联系云服务商对底层云硬盘执行“安全擦除”操作（非普通格式化），要求服务商提供云存储数据擦除报告（含擦除方法、检测结果），并留存报告归档；

c） 验证检测：删除完成后，使用专业数据恢复工具对存储介质进行抽样检测（抽样比例不低于30%），确认无原始数据残留。

7 数据治理

7.1 数据资源编目

7.1.1 编制方法

7.1.1.1 应建立数据源头识别机制，明确业务领域的第一性数据来源主体。当不同来源的数据发生冲突时，应由数据统筹部门依据业务权威性判定唯一源头，并建立数据溯源更正机制。在判定唯一源头时，应遵循“业务职能对齐”原则。对于基础空间地理数据，应以规划资源部门为权威源；对于法人及人口基础数据，应以政务数据库为权威源；对于行业运行监测数据（如水压、车次），应以业务系统原始记录为唯一源。若出现跨行业数据冲突，应由数据运营平台管理机构依据数据项的生成频率、采集精度及法定职权范围进行仲裁。

7.1.1.2 数据资源目录编制包括信息系统普查、数据资源目录梳理、数据资源目录审核、数据资源目录管理四个阶段，如图 2 所示。

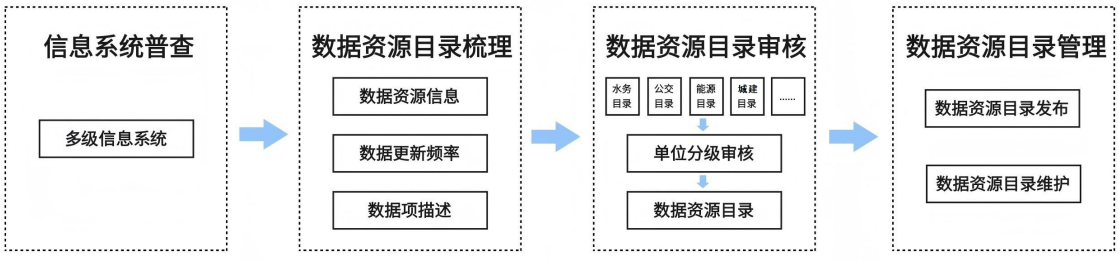

图2 数据资源目录编制流程图

7.1.2 信息系统普查

7.1.2.1 信息系统普查应覆盖城市运营涉及的各级管理主体及相关信息系统，确保目录编制的完整性。信息系统普查内容应包含以下要素：

a) 信息系统名称；
b) 系统所属单位；
c) 系统功能描述；
d) 系统状态，包括建设中、运行中、停用等；
e) 系统业务类型，包括门户网站、协同办公、数字驾驶舱、基础-服务存储、基础-网络安全、业务-公共服务、业务-经营管理、业务-生产运行、业务-应用场景；
f) 系统部署情况，包括自建机房、租用机房、云端等；
g) 系统网络环境，包括单位内网、业务专网、互联网等；
h) 系统访问地址；
i) 系统承建单位，包括承建单位、运维单位的公司名称、联系人、电话、邮箱、地址。

7.1.3 数据资源目录梳理

数据资源目录梳理应保证要素完整、内容规范准确。数据资源目录梳理内容应包含以下要素：
a) 数据资源名称；
b) 数据资源摘要；
c) 所属信息系统名称；
d) 更新频率：
e) 数据项描述：
1) 中文名称；
2) 英文名称；
3) 字段描述；
4) 数据类型；
5) 数据长度；
6) 是否字典项；
7) 是否可为空；
8) 是否主键；
9) 共享类型；
10) 共享条件；
11) 开放类型；
12) 安全级别。

7.1.4 数据资源目录审核

数据资源目录应进行分级审核，如图3所示。

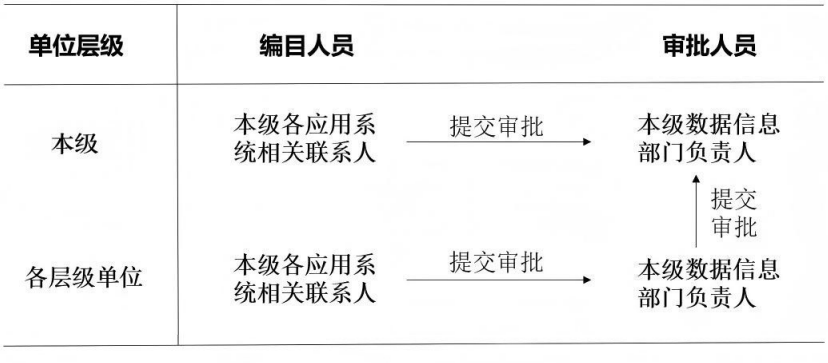

图3 数据资源目录审批流程图

7.1.5 数据资源目录管理

7.1.5.1 本级单位应对数据资源目录进行统一发布。
7.1.5.2 各层级单位主管部门应做好本级数据资源目录的更新与维护。

7.2 数据追溯

应建立城市运营服务数据可追溯机制，如通过审计日志等方式在采集、审核校验、更正等流程中进行唯一性标识，并对相关记录和文件进行归档。

8 数据质量管理

8.1 基本要求

应建立城市运营服务数据质量管理体系及实施机制,优化数据质量并持续改进,满足数据应用的求：

a) 建立数据质量管理机构和机制，明确数据质量管理的角色和职责，建立数据质量管理方法；
b) 明确不同数据之间的关系和依赖性，制定数据质量管理目标；
c) 识别数据生存周期各个阶段的数据质量元素，构建数据质量评估框架；
d) 采用定性评估、定量评估或综合评估等方法，评估和持续优化数据质量；
e) 建立数据管理质量管理记录。

8.2 数据标准

8.2.1 数据标准是一组经过协商一致的、对数据的结构、内容、格式、质量、安全等方面做出的统一规定和要求。数据标准旨在确保不同系统、不同部门、不同用户之间对数据的理解和使用保持一致。

8.2.2 数据标准管理应涵盖两个方面核心内容：基础数据标准、指标数据标准。

8.2.3 基础数据标准通常涵盖三个关键部分：

a) 业务属性：主要描述基础数据的业务层面信息，包括标准主题、标准分类、标准编码、标准中英文名称、业务定义、业务规则、相关标准引用、标准来源和依据；
b) 技术属性：关注基础数据的技术细节，确保数据能够在系统中得到正确实现，包括数据类型、数据格式、长度、编码规则、取值范围等；
c) 管理属性：涉及数据的治理和管理澄面，包括数据的标准定义者、管理者、使用者，以及数据标准的版本，应用领域，所服务的系统等。

8.2.4 指标数据标准在实体数据的基础上，通过增加统计维度、计算方法和分析规则等信息加工而成的数据。涉及对业务指标的统一定义和管理，与基础数据相似，也分为业务属性、技术属性和管理属性三个部分：

a) 指标业务属性：涉及指标的具体业务内容，包括指标编码、中英文名称、主题、分类、类型、业务定义、业务规则、数据来源、取数规则、统计维度、计算公示、显示精度以及相关基础数据标准等；
b) 指标技术属性：描述指标的技术细节，包括指标来源系统、使用系统、数据源表、数据类型、度量单位、取值范围、生成频度、计算周期、取数精度等；
c) 指标管理属性：涉及指标的管理信息，如归口部门、业务负责人、技术负责人、指标权限范围等。

8.3 数据质量

8.3.1 数据质量应通过制定数据标准来进行保证。

8.3.2 数据质量评价方法可分为定性评价法和定量评价法：

a) 定性评价法可根据事先确定的评价指标，对数据的安全性、目的、用途、日志以及用户自定义项目进行评价；
b) 定量评价法可采用数据质量检测软件检查数据质量，也可通过辅助工具结合人工识别分析方法进行人工检查。一般可分为全数检查和抽样检查：
   1) 针对国家强制要求、特殊要求、其他可能导致严重影响的数据质量项目进行全数检查；
   2) 针对质量比较稳定、数据量较大、检查费用与时间有限的情况进行抽样检查。

8.3.3 数据质量主要包括规范性、完整性、准确性、唯一性、一致性、时效性和可访问性等方面，数据质量要求应符合表 1 的规定。

表1　数据质量要求

一级指标	二级指标	要求
规范性	命名规范	数据库、数据表、数据字段等应按照国家标准、行业标准、地方标准等规定的统一规则命名
	数据类型规范	数据实际类型应与国家标准、行业标准、地方标准等规定的类型格式保持一致
	数据值域规范	数据的取值范围应与国家标准、行业标准、地方标准等规定的值域代码表保持一致
规范性	精度规范	对于数字型数据，应按照国家标准、行业标准、地方标准等规定的精度进行填写
	计量单位规范	对于存在计量单位的数据，应按照国家标准、行业标准、地方标准等规定的计量单位进行填写
准确性	数据合理	数据值应符合业务逻辑，不应存在逻辑或常识性错误
	数据符合预期	数据值应与数据集、数据字段名称保持一致，不应出现预期外的数据
完整性	数据记录完整	数据应包含完整的数据记录，不应存在缺失、遗漏
	数据字段完整	数据应包含完整的数据字段，不应存在缺失、遗漏
	数据值完整	若数据具有主键，其主键值应完整，不应为空或缺失；基于业务规则应被赋值的数据值应完整
唯一性	主键唯一	数据的主键应唯一，不应重复
	字段唯一	数据的字段应唯一，不应重复
	记录唯一	数据的记录应唯一，不应重复
一致性	相同数据一致	对于存储在不同位置的同一数据应保持一致，当数据发生变化时，存储在不同位置的数据应同步更新
	关联数据一致	对于存在关联关系的数据，当数据发生变化时，其关联数据应同步更新
时效性	更新及时性	对于基于时间段记录的数据和基于时间点记录的数据，应按照规定的更新频率进行更新
	时序合理	数据之间的相对时间顺序应符合逻辑
可访问性	数据可访问	数据应在需要时可被有效获取

9　数据安全管理

9.1　基本要求

城市运营服务数据安全应符合GB 17859、GB/T 22239、GB/T 22240、GB/T 37025、GB/T 39477等对数据安全的要求。

9.2　访问安全

9.2.1　根据数据的保密要求限定访问源，敏感数据应只接受来自内网、专线或虚拟专网的访问请求，并通过加密或其他有效措施实现传输保密性。

9.2.2　应采用白名单机制,对数据库的访问权限进行细粒度控制,只允许特定的客户端进行访问,减少潜在的风险和安全漏洞。

9.2.3　数据访问应采用三层次认证体系，包括身份认证、访问权认证和操作权限认证。

9.2.4　数据访问应通过设置角色、权限等方式实现对用户操作数据的限制，保护敏感信息或商业机密的数据不被非法访问和恶意篡改。

9.3　加工安全

9.3.1　对于高性能、高密级数据的加工，应通过隐私计算工具。部署供需侧分布式计算节点，保障在数据不出域的情况完成数据加工计算。

9.3.2　用户应在可信空间内处理核心敏感数据。

9.3.3　应通过资源软隔离技术划分不同项目组的资源，避免相互干扰。

9.3.4 用户访问数据时，应通过字段级权限控制，确保其只能看到被授权部分的明文或脱敏结果。
9.3.5 当用户经审批后导出结果数据时，系统应自动注入数据水印，以便未来可能需要的追溯。

9.4 存储安全

9.4.1 对于特定的敏感字段或业务数据应使用加密存储。
9.4.2 存储在非生产环境(如测试、开发、分析库)中的数据应进行静态脱敏。
9.4.3 除对数据本身进行备份外，还应备份数据配置信息、数据维护日志、系统访问日志及数据访问日志等。
9.4.4 应定期对数据做增量备份及全量备份，数据备份应保存两个以上版本，全量备份应在访问量较小的时段进行。
9.4.5 应支持手工备份和自动备份两种方式，备份策略配置灵活。
9.4.6 数据应能够在线备份，在不间断服务的情况下完成备份。
9.4.7 备份对象应能够按既定的备份策略备份到指定介质。

9.5 使用安全

9.5.1 根据数据的不同特征和业务需求，应对数据进行实时动态的脱敏处理。
9.5.2 在数据使用阶段，特别是数据外发和导出时，应自动注入数据水印。
9.5.3 应开展安全审计，审计范围应覆盖业务数据的全部用户行为，审计记录应包括事件的时间、类型、主客体标识和结果等，并保证审计记录不被删除或篡改。
9.5.4 当访问源可控且固定，尤其是涉及内部系统、第三方集成和高危操作时，应采用接口白名单。