

交通运输非涉密数据安全分级与防护
技术规范

Technical specifications for security classification and protection
of non-confidential transportation data

2025 - 12 - 15 发布

2026 - 03 - 15 实施

目 次

前言..... III

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 数据安全分级方法..... 2

 4.1 分级原则..... 2

 4.2 分级级别..... 2

 4.3 分级要素..... 2

 4.4 安全风险分析..... 3

 4.5 分级方法..... 3

 4.6 分级步骤..... 4

 4.7 数据级别适时调整..... 5

5 数据安全防护技术要求..... 6

 5.1 防护原则..... 6

 5.2 安全防护技术要求..... 6

附录A（规范性） 数据分级..... 9

附录B（资料性） 交通领域数据分级参考示例..... 10

附录C（资料性） 个人信息去标识化脱敏参考示例..... 13

参考文献..... 14

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。

本文件由湖南省交通运输厅提出并归口。

本文件起草单位：湖南省交通运输厅科技信息中心、浩鲸云计算科技股份有限公司、奇安信网神信息技术（北京）股份有限公司、湖南交通职业技术学院、湖南食品药品职业学院。

本文件主要起草人：颜志欣、王方、单新周、聂皓冰、张岸杨、毛恒彬、罗文、王冉然、刘洋、肖磊、杨慧芳、杨常烨、周禹、张志强、景亮、楚赟、周武宁。

交通运输非涉密数据安全分级与防护技术规范

1 范围

本文件规范了交通运输非涉密数据的安全分级方法、各级别数据的安全防护技术要求。
本文件适用于公路、水路、道路运输、城市交通等交通运输行业非涉密数据安全分级和防护管理。

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 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 35273 信息安全技术 个人信息安全规范
- 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 39204 信息安全技术 关键信息基础设施安全保护要求
- GB/T 43697 数据安全技术 数据分类分级规则
- GB/T 45574 数据安全技术 敏感个人信息处理安全要求
- JT/T 1522-2024 交通运输数据安全分级和保护要求
- DB43/T 3093 湖南省交通运输政务信息资源目录编制规范

3 术语和定义

GB/T 43697、GB/T 45574、JT/T 1522界定的以及下列术语和定义适用于本文件。

3.1

非涉密数据

不属于《中华人民共和国保守国家秘密法》规定的国家秘密信息，可依法公开或共享的数据。

3.2

数据处理者

对交通运输非涉密数据进行存储持有、加工使用、传输提供的责任主体。

注：数据处理者包括：

- a) 业务部门：数据的产生方或权属方，负责主导数据分级决策与使用审批；
- b) 技术支持方：受业务部门委托提供技术服务的组织或个人，负责执行分级防护的技术措施。

[来源：JT/T 1522-2024，3.1.1，有修改]

3.3

数据集

数据记录汇聚的数据形式。

注：它可以具有大数据的体量、速度、多样性和易变性特征。数据集的特征表征的是数据本身或静态数据，而数据的特征，当其在网络上传输时或暂时驻留于计算机存储器中以备读出或更新时，表征的是动态数据。

[来源：GB/T 35295-2017，2.1.46，有修改]

3.4

关键信息基础设施

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源：GB/T 39204-2022，3.1]

4 数据安全分级方法

4.1 分级原则

交通运输数据（以下简称数据）安全分级原则按JT/T 1522-2024第4.1条款执行。

4.2 分级级别

数据安全级别分为核心数据、重要数据、一般数据（见附录A），并补充以下要求：

- a) 公共数据的开放/共享级别应符合：
- 1) 有条件开放/共享的数据安全级别不低于一般2级数据；
 - 2) 禁止开放/共享的数据安全级别不低于一般3级数据。

4.3 分级要素

影响数据分级的要素，包括数据的领域、群体、区域、精度、规模、深度、覆盖度、重要性。其中领域、群体、区域、重要性通常属于定性描述的分级要素，精度、规模、覆盖度属于定量描述的分级要素，深度通常作为衍生数据的分级要素。识别数据定级要素相关情况，常见考虑因素见表1。

表1 数据安全分级要素

要素名称	要素释义	常见要素及举例
领域	数据描述的业务或内容范畴。	可结合DB43/T 3093-2024 5.3信息资源分类，明确数据所涉及的行业领域和业务领域。 1. 行业领域，如道路运输、公路交通、水路交通等行业。 2. 业务领域，如城市公交业务、公路建设业务、道路货运等业务。
群体	数据主体或描述对象集合。	1. 人群，如道路运输从业人员基本信息。 2. 团体、单位、组织，如道路运输经营业户信息、项目施工单位信息。 3. 项目，如公路建设项目、水运建设项目信息。 4. 设备，如交通应急设备、公路监控设备信息。
区域	数据涉及的地区范围。	1. 行政区划，如湖南省营运车辆基本信息、长沙市公交车信息。 2. 特定区域，如许广高速湖南段门架通行数据。 3. 重要场所数据，如湖南省相关行业政府机构信息。
精度	数据精度越高标识采集数据和真实数据的误差越小。	1. 定位精度，如米级位置定位数据。 2. 地图精度，如精度和比例尺优于开放标准的地图数据。 3. 图像清晰度，如高速公路摄像头采集的720P视频。 4. 时间精度，如传感设备的毫秒级时间戳。 5. 数值精度，如高速收费交易金额精确到分。

表1 数据安全分级要素（续）

要素名称	要素释义	常见要素及举例
规模	数据规模及数据描述的对象范围或数量大小。	1. 数据存储量，如公路养护数据规模 10GB。 2. 数据共享规模，如从业资格证数据每月共享规模 2GB。 3. 交易量，如 MTC/ETC 车道日均交易 50 万笔。 4. 群体规模，如公路建设项目个数、车载视频设备台数。
深度	对数据描述对象的隐含信息挖掘的触达程度，或多维度细节信息的刻画程度。	1. 动态轨迹，如包含“车牌号、经度、纬度、定位时间”的数据，与包含“车牌号、经度、纬度、定位时间、车速、方向、海拔高度”的数据深度不同。 2. 个人信息，如包含“姓名、生日、性别、国籍、民族、家庭住址”的数据，与包含“姓名、生日、性别、国籍、民族、家庭住址、手机号、固定电话、邮箱地址”的数据深度不同。
覆盖度	数据对领域、群体、区域、时段等的覆盖分布或疏密程度。	1. 领域覆盖占比，如公路上的监控设备覆盖了总里程的 90%。 2. 群体覆盖占比，如长沙市网约车从业人员数量覆盖全湖南省网约车从业人员的比例。 3. 区域范围，如长沙全市公交车运行数据。 4. 时段覆盖度，如高速收费站 ETC 交易流水数据全天 24 小时覆盖；历史数据的覆盖分布；
重要性	数据在经济社会发展中的重要程度。	1. 判断数据是否可能影响社会稳定，可能引发社会恐慌，导致重大突发事件、群体性事件、暴力恐怖活动、社会治安问题等； 2. 判断数据是否可能影响行业领域或地区的经济发展、业务生产、技术进步、产业生态等。 3. 判断数据是否可能影响公共场所的活动秩序、公共交通秩序。

4.4 安全风险分析

数据安全风险分析按JT/T 1522-2024第4.4条款执行。

4.5 分级方法

4.5.1 基本分级规则

基本分级规则按JT/T 1522-2024第4.5.1.1、4.5.2.1条款执行。

4.5.2 数据级别与安全风险的判定关系

数据级别与安全风险的判定关系按JT/T 1522-2024第4.5.1.2、4.5.2.2条款执行。

4.5.3 个人信息分级规则

如果数据包含个人信息，其数据分级在遵循4.5.1和4.5.2的基础上，还应遵循以下规则：

- a) 100万人以上的个人信息数据集首先判定是否为重要数据、核心数据，如不属于重要数据，其数据集的安全级别不低于一般3级数据；
- b) 除JT/T 1522-2024附录A个人信息识别及参考示例，其他个人信息是否敏感需按《中华人民共和国个人信息保护法》第二十八条评估危害后果判定，敏感个人信息数据安全级别不低于一般3级数据；
- c) 经匿名化处理（符合GB/T 37964《信息安全技术 个人信息去标识化指南》）且无法复原关联性的数据，按非敏感个人信息进行分级管理，非敏感个人信息数据安全级别通常不低于一般2级数据。

4.5.4 地理信息定级规则

如果数据包含地理信息，其数据分级在遵循4.5.1和4.5.2的基础上，还应遵循以下规则：

- a) 当数据满足以下任意一项时，应识别为重要数据：
 - 1) 军事禁区以外连续覆盖范围不超过25平方公里，但累计达到较高覆盖度或较大规模的大于1:5千的国家基本比例尺地形图数据、平面精度优于10米或者地面分辨率优于0.5米的正射影像数据、平面精度优于（含）10米或高程精度优于（含）15米的数字高程模型和数字表面模型数据以及平面精度优于（含）10米或地物高度相对量测精度优于（含）5%的三维模型、点云、倾斜影像、实景影像、导航电子地图等数据；
 - 2) 体现重要目标、重要场所、关键交通基础设施内部详细构造等信息的三维模型数据；
 - 3) 覆盖全省区域范围的1:1万公众版矢量数据；
 - 4) 覆盖全省，规模大且极具敏感性、重要性的地理信息数据，或直接影响关键信息基础设施正常运行服务的地理信息数据；
 - 5) 达到一定规模，能够反映政府机关、军事设施、重要科研机构工作人员等特定群体画像、准确定位和细粒度时空规律，或能够反映我国战略储备、应急动员、作战等能力以及重点领域产业链供应链等情况的经匿名化处理后的位置轨迹数据。
- b) 基础定级规则根据地理信息数据的特性和精度，按以下描述确定级别：
 - 1) 数据集包含关键交通基础设施的地理坐标，且误差绝对值小于0.5米，其安全级别不低于一般3级数据；
 - 2) 数据集包含关键基础设施以外的其他路段的地理坐标，且误差绝对值小于0.5米，其安全级别不低于一般2级数据。

4.5.5 衍生数据分级规则

衍生数据分级规则按JT/T 1522-2024第4.5.4条款执行。

4.6 分级步骤

4.6.1 数据分级流程

数据处理者开展数据分级工作时，应在遵循国家和行业领域数据分类分级要求的基础上，参考以下步骤开展数据分类分级工作：

- a) 数据资产梳理：对数据资产进行全面梳理，确定待分级的数据资产及其所属的行业领域。
- b) 制定内部细则：按照行业领域数据分级标准规范，结合处理者自身数据特点，参考本文件按需制定自身的数据分级细则。
- c) 实施数据分级：数据分级步骤，确定数据的安全级别及其具体范围。
 - 1) 确定分级对象：确定待分级的数据，如数据项、数据集、衍生数据等；
 - 2) 分级要素识别：结合自身数据特点，按照4.3识别数据涉及的分级要素情况。
 - 3) 安全风险分析：结合数据要素的识别情况，分析数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，可能产生的影响（见4.4）。
 - 4) 综合确定级别：依次判定数据是否为重要数据、核心数据、一般数据，按照4.5，综合确定数据级别。数据分级样例参考附录B。
- d) 数据级别适时调整：根据数据重要程度和可能造成的危害程度变化，按照4.7，对数据分级规则、重要数据和核心数据目录、数据分级清单和标识等进行适时调整。

4.6.2 数据分级步骤示意图1

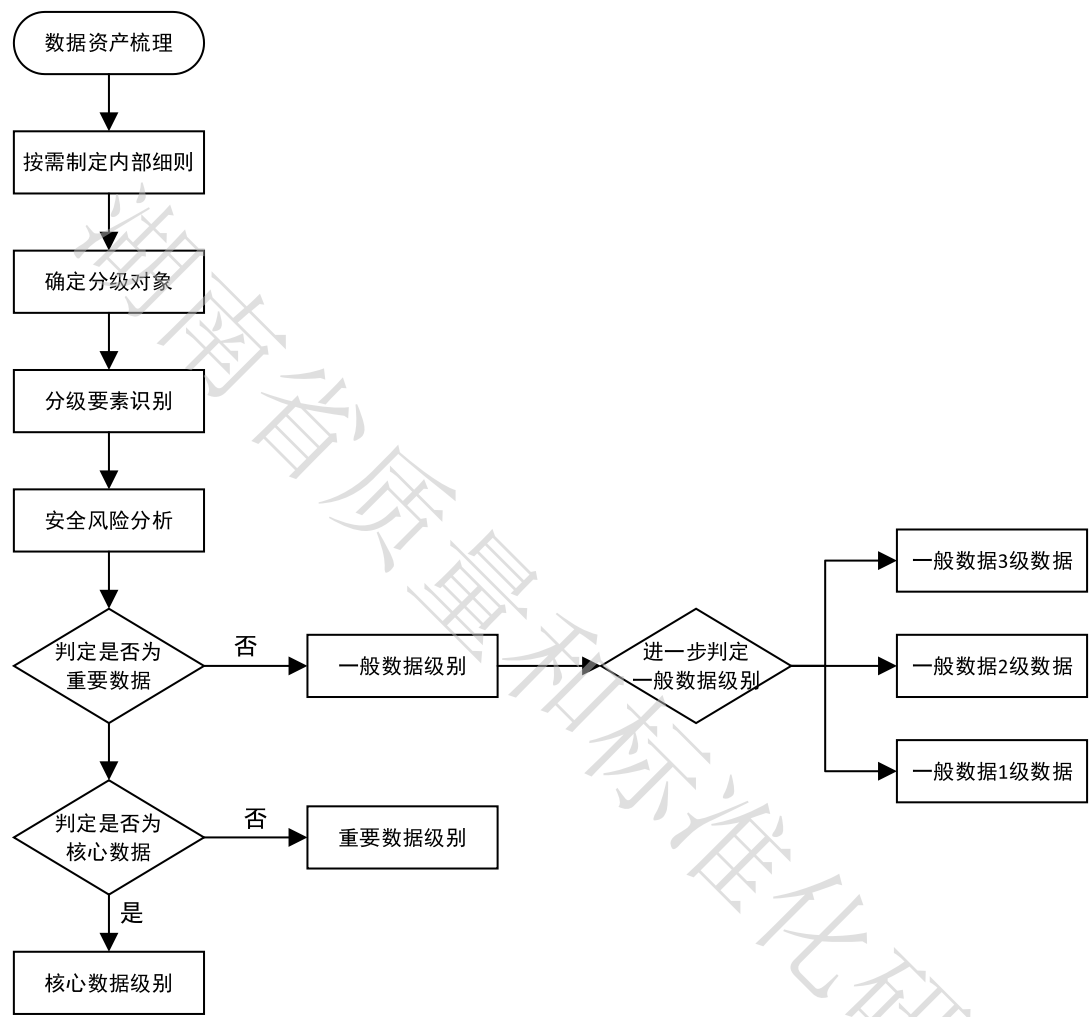


图1 数据分级步骤

4.7 数据级别适时调整

数据级别确定后，出现下列情形之一时，应对数据级别进行调整：

- a) 数据内容发生变化，导致原定的数据级别不再适用；
- b) 数据内容未发生变化，但数据时效性、数据规模、数据应用场景、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) 多个原始数据直接合并，导致原定的数据级别不再适用于合并后的数据；
- d) 因对不同数据选取部分数据进行合并形成新的数据，导致原定的数据级别不再适用于合并后的数据；
- e) 不同数据类型经汇聚融合形成新的数据，导致原定的数据级别不再适用于汇聚融合后的数据；
- f) 数据进行脱敏或删除关键字段，或者经过去标识化、匿名化处理的数据；
- g) 发生数据安全事件，导致数据敏感性发生变化；
- h) 因国家、安全监管部门或交通行业主管部门要求，导致原定的数据级别不再适用。

5 数据安全防护技术要求

5.1 防护原则

数据安全防护依据数据安全级别采用分级防护，防护措施应贯穿数据处理各环节，遵循“合法正当、目的明确、最小必要、就高从严”的原则。

5.2 安全防护技术要求

5.2.1 一般1级数据

一般1级数据的安全防护技术规范遵循JT/T 1522-2024第5.3.1条款的规定，并补充以下规范要求：

- a) 数据收集：明确目的、用途、数据源和收集频度，涉及个人信息收集应获得个人信息主体的授权同意并确认授权范围；对数据源、数据收集终端、数据导入服务组件等使用进行身份鉴别。应对收集数据的完整性进行验证；对数据收集环境和设施采取安全管控，并对数据收集过程进行详细日志记录，确保收集操作可追溯。
- b) 数据存储：不存储非业务所需数据，存储时长为满足业务需求的最短时间；在中国境内收集和产生的数据需存储在中国境内，并设置访问控制、时效管理等安全措施。数据分域存储，对生产环境、测试环境等进行有效隔离；对分布式处理过程中不同数据副本节点数据的完整性和一致性应定期检测；定期开展数据恢复测试和灾难恢复演练，对备份数据的有效性和可用性进行检查和恢复验证。
- c) 数据使用与加工：应在数据收集声明或授权范围内使用、加工数据，对于超范围使用个人信息的情况要再次获得用户的明确同意；应针对不同等级的数据设置不同的访问权限，不同用户只能访问自己权限对应的数据。
- d) 数据传输：数据传输应采用安全可信通道、安全协议以及数据加密等手段，保障通信过程中数据的可用性机密性与完整性。具备对传输数据的完整性进行校验的能力，并提供相应的恢复控制措施；应具备链路冗余、断点续传和超时重连能力，符合数据传输任务的可靠性要求。
- e) 数据提供：数据提供前开展数据安全影响评估，对提供的数据内容、数据安全级别、数据范围、时间周期、数据保存期限、传输方式、用途、安全管控手段等要素进行评估。在数据提供前应经过审批并与数据获取方签订数据处理协议；数据提供过程中对数据采取相应防护措施（如脱敏、加密风险监测和预警、日志记录与审计等），以保障数据提供过程的安全。脱敏参见附录C。
- f) 数据公开：数据公开前对数据公开的必要性、范围、规模和方式进行分析评估，并审核公开的合规性。数据公开应通过官方渠道进行，同时利用防篡改等技术保障公开数据的完整性，记录公开行为日志。
- g) 数据删除和销毁：通过文件删除、数据覆盖（单次）的方式对数据进行删除。对于数据删除、销毁，建立审批机制并保留审批记录。依据实际情况制定数据删除、销毁策略，明确界定销毁场景、对象、要求和流程。并建立存储介质销毁的有效性评估、复核、抽样认定等机制，对销毁记录定期检查。

5.2.2 一般2级数据

在满足一般1级数据安全防护技术规范的基础上，一般2级数据的安全防护技术规范遵循JT/T 1522-2024第5.3.2条款的规定，并补充以下规范要求：

- a) 数据收集：应采用数据标识、日志记录、水印等技术措施对数据来源进行记录，实现安全域外溯源。一般1级及以上数据应实现安全域内溯源。
- b) 数据传输：应采用安全传输通道、安全传输协议进行数据安全传输，因技术或协议本身限制无法确保数据传输安全时，数据应加密后传输或实施网络隔离并通过白名单控制。
- c) 数据提供：应采用行为监测、分析等技术措施对异常和高风险数据共享行为进行自动化识别和实时预警。
- d) 数据公开：应进行脱敏后公开，确需直接对其进行非脱敏的共享时，应获得个人信息主体的授权同意，经审批后共享；或进行可用不可见的共享。脱敏参见附录C。
- e) 数据删除和销毁：应采用多次覆写等方式安全擦除数据，以防止数据被恢复或再次利用，若存储介质因故障无法进行数据擦除或不再使用，则需采用消磁、焚烧、粉碎等不可恢复的方式予以销毁。

5.2.3 一般3级数据

在满足一般2级数据安全防护技术规范的基础上，一般3级数据的安全防护技术规范遵循JT/T 1522—2024第5.3.3条款的规定，并补充以下规范要求：

- a) 数据收集：应仅在个人信息主体使用业务功能期间，收集该业务功能所需的敏感个人信息；应向个人信息主体告知个人信息处理者的名称或姓名、联系方式等基本情况，敏感个人信息的处理目的、处理方式和必要性，敏感个人信息的种类、保存期限和对个人权益的影响，个人信息主体行使个人信息主体权利的方式和途径。
- b) 数据存储：使用业界公开的或国家发布的安全加密算法保证存储数据的机密性，不应使用私有加密算法；敏感个人信息与可识别个人身份的信息分开存储，去标识化的敏感个人信息与可用于恢复识别个人的信息分开存储。
- c) 数据使用与加工：数据使用默认应脱敏显示（脱敏参见附录C），如因业务需要查看明文，应提供单独的查看功能，并使用多因素认证或二次授权机制；应严格限制敏感个人信息访问权限和有效期，敏感个人信息权限申请和使用应基于业务需要，且仅授予访问其业务所必须的最少敏感个人信息类型和数量。
- d) 数据传输：采用数字签名、时间戳等方式保证抗抵赖性。采取准入控制、终端鉴别等技术措施，防止非法或未授权终端接入内部网络。
- e) 数据公开：不宜直接公开原始数据，若因业务活动需要公开，应事先进行风险评估，并将评估结果报主管部门备案。经审批后进行公开，并留存记录。数据公开发布后，需定期检查公开发布的数据中是否含有非公开信息。
- f) 数据删除和销毁：通过数据覆盖（至少三次）、安全擦除的方式对数据进行删除。宜对敏感个人信息删除或匿名化处理效果进行评估，已删除或匿名化处理的敏感个人信息不应被还原；应建立敏感个人信息删除机制并提供个人信息主体删除其敏感个人信息的便利机制，法律和行政法规规定需要留存敏感个人信息的，应在到期后及时删除或匿名化处理。

5.2.4 重要数据

在满足一般3级数据安全防护技术规范的基础上，重要数据的安全防护技术规范遵循JT/T 1522—2024第5.3.4条款的规定，并补充以下规范要求：

- a) 数据存储：对数据字段采用符合国家要求的密码算法进行加密存储，并对加密数据密钥进行严格管理，包括密钥存放位置、方式、密钥更换周期等。
- b) 数据提供：确需因业务需要向境外提供时，应向国家网信部门申报并通过数据出境安全评估。

- c) 数据删除和销毁：设置数据销毁相关监督人员，对销毁过程进行监督。存储介质的物理销毁应确保销毁前数据彻底删除。当涉及云存储时，应使用相关工具，对数据进行彻底清除。采用国家权威机构认证的设备对存储介质进行销毁，或由专业机构进行数据销毁工作。
- d) 全过程处理：对数据处理进行全程记录和监控审计。如按国家和行业数据分类分级保护有关规定，达到一定规模的敏感个人信息被认定为重要数据，应按重要数据进行保护。

5.2.5 核心数据

核心数据的安全防护技术规范按JT/T 1522-2024第5.3.5条款执行。

附 录 A
(规范性)
数据分级

表A.1参考GB/T 43697、JT/T 1522-2024给出了数据分级级别和典型数据示例。

表A.1 数据分级

代码	数据级别	说明
1	一般 1 级数据	除重要数据、核心数据以外的，一旦遭到泄露、篡改、毁损、非法使用或共享，不会对个人和组织合法权益造成危害的数据。数据具有公共传播属性，可对外公开发布、转发传播，但也要考虑公开的数据量及类别，避免由于类别较多或者数据量过大被用于关联分析。 例如：依法依规公开、公示后的个人违规、违法等内容及超过一年以上的个人行踪数据；记录时间、数据 ID 等不涉及信息主体的数据。
2	一般 2 级数据	除重要数据、核心数据以外的，一旦遭到泄露、篡改、毁损、非法使用或共享，可能对个人或组织合法权益造成轻微危害的数据。数据通常在组织内部、关联方共享和使用，相关方授权后方能向组织外部共享。 例如：姓名、生日、性别、国籍、民族、手机号、固定电话、邮箱地址、通信地址等个人基本信息，教育工作信息等个人基本信息。
3	一般 3 级数据	除重要数据、核心数据以外的，一旦遭到泄露、篡改、毁损、非法使用或共享，可能对个人或组织合法权益造成严重危害的数据，或者可能对经济运行、社会稳定、公共健康和公共安全造成轻微危害。数据仅允许由授权的内部机构或人员访问，如果要将数据共享到外部，需经过严格审批、评估后才能够共享或传播。 例如：个人的家庭住址、身份证鉴别信息、轨迹位置信息、未公开的违法信息、生理健康信息等敏感个人数据。
4	重要数据	一旦遭到泄露、篡改、毁损、非法使用或共享，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的的数据。重要数据不包括涉及国家秘密的数据，仅影响组织自身或公民个人的数据一般不作为重要数据。
5	核心数据	一旦遭到泄露、篡改、毁损、非法使用或共享，可能直接危害政治安全的重要数据，以及对国家安全其他领域安全造成严重危害的重要数据。

附录 B

(资料性)

交通领域数据分级参考示例

表B.1给出了交通领域数据分级参考示例，因数据规模、数据应用场景不同，实际应用时参考4.7对数据级别进行适时调整。

表B.1 交通领域数据分级参考示例

行业领域	信息资源名称	数据描述	建议级别	建议理由
公路交通	公路路线基本情况明细	主要包括路线名称，技术等级名称，起点名称，止点名称，起点桩号，止点桩号，起点经纬度，止点经纬度，管养单位名称，设计时速，路基宽度，路面宽度，车道数量，面层厚度等。	一般3级	包含满足一定精度指标的地理信息，重要业务数据。
	高速收费站	主要包括收费站名称，收费站类型名称，坐标纬度，坐标经度，所在区县编码，桩号等。	一般2级	包含满足一定精度指标的地理信息。
	MTC/ETC 车道入口流水	主要包括 CPC 卡或 ETC 卡的编号，CPU 卡片网络编号，OBU 编码，PSAM 卡脱机交易序列号，入口收费公路编号，入口收费站 HEX 码，入口日期及时间，入口站编号，入口识别车辆车牌号码+颜色，班次流水号，车牌识别流水号，车辆识别标识等。	一般3级	包含个人财产信息、其他个人基本信息。
	项目信息	主要包括项目名称，工程概算，工程结算，建设内容，建设单位名称，总承包商统一社会信用代码，施工单位统一社会信用代码，施工许可证号，法定代表人，负责人电话，项目负责人等。	一般2级	包含个人基本信息。
	公路建设信用-企业资质信息	主要包括业务承接范围，发证日期，发证机关，审核状态，所属专业/专项，所属行业名称，等级，统一社会信用代码，资质证书编号等。	一般1级	可公开的企业信息。
	公路建设信用-人员职称信息	主要包括统一社会信用代码，职称专业，职称名称，职称核发日期，职称核发机关，职称级别，职称证书编号，身份证号等。	一般2级	包含个人身份信息。
	企业财务信息	主要包括主营业务利润率，主营业务收入，公路工程总收入，净利润，净资产，净资产收益率，利润总额，固定资产，总资产，总资产报酬率，水运工程总收入，注册资金，流动比率，流动负债，流动资产，现金流量净额，组织机构代码，统一社会信用代码，营业收入，负债总额，资产负债率，银行授信等级，银行授信额度等。	一般3级	包含重要业务数据。
	湖南高速公路事件信息	主要包括路线名称，路段名称，阻断位置，阻断原因分类，阻断发生区域，纬度，经度，发现时间，发生时间，起点桩号，止点桩号等。	一般2级	包含满足一定精度指标的地理信息。
水路交通	运输船舶名录	主要包括主机合计功率，净载重量，名录序号，型宽，总载重量，总长，满载吃水，箱位数，航速，船名，船检登记号，船舶总吨，船舶经营人，载客量等。	一般2级	包含其他个人基本信息。
	渡口年报信息	主要包括填报单位，填报单位负责人，填表人，填表人电话，审核人，审核人电话，建成时间，是否机动渡口，渡口名称，渡口宽度，渡口类型，渡口纬度，渡口经度等。	一般2级	包含满足一定精度指标的地理信息，个人基本信息。

表B.1 交通领域数据分级参考示例（续）

行业领域	信息资源名称	数据描述	建议级别	建议理由
水路交通	水路安全-航标信息	主要包括航标名称, 航标编码, SIM 卡号, X 方向加速度, Y 方向加速度, Z 代表重力方向竖直向下, 基准纬度, 基准经度, 安全作用距离, 当前电量, 所属单位名称, 所属航道名称, 放电电量, 日光阈值, 材质, 标形, 标志位置, 漂移距离, 灯质, 维护人员, 负载电压, 负载电流等。	一般 3 级	包含满足一定精度指标的地理信息。
	水运工程建设市场信用-企业登记信息	主要包括单位名称, 单位联系人, 单位负责人姓名, 单位负责人联系电话, 单位负责人身份证号, 基本账户开户银行, 基本开户账户, 安全生产许可证发证单位, 安全生产许可证编号, 安全生产许可证许可范围, 安全生产负责人姓名, 安全生产负责人身份证号, 安全许可证号码, 技术负责人, 技术负责人联系电话, 技术负责人身份证号, 曾用名, 法定代表人, 法定代表人, 法定代表人联系电话, 法定代表人身份证号, 社保登记证编号, 税务登记证编号, 联系人电子邮箱, 联系人电话等。	一般 3 级	包含敏感个人信息。
	水路运政管理人员名录	主要包括姓名, 性别, 职务, 资格证书名称, 类别, 等级等。	一般 2 级	包含个人基本信息。
	水路运输客货运月指标	主要包括指标编码, 指标值, 指标名称, 指标单位, 区域代码, 统计年份, 统计月份等。	一般 1 级	可公开的统计信息。
道路运输	道路运输营运车辆基本信息	主要包括注册登记日期, 车辆吨位, 车辆准牵引总质量, 车辆车轴数, 车辆车高, 车辆车宽, 车辆车长, 车辆燃料类型代码, 出厂日期, 车辆识别码, 发动机号, 车辆厂牌型号, 车辆厂牌, 车辆地行政区域代码, 车辆状况, 车辆类型, 车牌颜色, 车辆号牌, 经营业户等。	一般 2 级	包含其他个人基本信息。
	从业人员基本信息	主要包括从业人员户籍地行政区划, 身份证件类型, 技术职称, 性别, 民族, 驾驶证有效期止, 驾驶证有效期起, 国籍, 准驾车型, 驾驶证号, 驾驶证初领日期, 出生日期, 从业人员状况代码, 从业人员状况, 文化程度, 联系地址, 联系电话, 身份证号, 姓名等。	重要数据	包含敏感个人信息, 数据量超过 100 万条。
	人员履职信息	主要包括入职时间, 准驾车型, 创建人姓名, 参加社保情况, 在职状态, 头像, 头像外部地址, 家庭住址, 工作经历, 异动情况, 所属公司(承运商), 政治面貌, 文化程度, 最后更新人姓名, 毕业院校, 民族, 结婚状态, 邮箱, 驾驶证号等。	一般 3 级	包含敏感个人信息。
	道路运输经营业户基本信息	主要包括法人身份证号, 法人, 统一社会信用代码, 经营业户电话号码, 经营业户负责人电话号码, 经营业户负责人姓名, 业户地址, 经营业户名称等。	一般 2 级	包含个人基本信息。
	道路运输证信息	主要包括车辆状态, 初次发证日期, 经营范围, 发证机构, 所属业户, 发证机关区域代码, 道路运输证号车牌颜色等。	一般 2 级	包含其他个人基本信息。
	道路运输车辆定位信息	主要包括经纬度, 海拔高度, 车牌号, 车牌颜色, 车辆状态信息, 定位速度、行驶记录速度、车辆当前里程数、方向、平台接入码、定位时间。	一般 3 级	包含满足米级位置定位数据
	报警处置信息	主要包括处置时间, 处置状态, 处置结果, 报警原因, 报警时间, 纬度, 经度, 车牌号等。	一般 2 级	包含满足一定精度指标的地理信息, 其他个人信息。

表B.1 交通领域数据分级参考示例（续）

行业领域	信息资源名称	数据描述	建议级别	建议理由
城市交通	网约车平台公司基本信息	主要包括公司名称，法人代表姓名，法人代表电话，法人代表身份证号，注册资本，经营范围，通信地址等。	一般 2 级	包含个人基本信息。
	网约车驾驶员定位信息	主要包括公司标识，坐标加密标识，定位时间，方向角，机动车驾驶证号，海拔高度，瞬时速度，纬度，经度，营运状态，行政区划代码，订单编号，车辆号牌等。	一般 3 级	包含敏感个人信息。
	网约车乘客基本信息	主要包括乘客性别，乘客手机号，乘客称谓，公司标识，市州行政区划代码等。	一般 2 级	包含个人基本信息。
	网约车经营支付信息	主要包括 POS 机支付机构，POS 机支付金额，上车地点，上车时间，下车地点，下车时间，乘客结算时间，优惠金额，公司标识，实收金额，实际使用车型，市州行政区划代码，应收金额，机动车驾驶员姓名，机动车驾驶证号，现金支付金额，电子支付机构，电子支付金额，空驶里程，等待时间，结算状态，订单完成时间，订单编号，车辆出发纬度，车辆出发经度，车辆到达纬度，车辆到达经度，车辆号牌，载客时间，载客里程，附加费等。	一般 3 级	包含敏感个人信息。
综合管理	行政执法人员	主要包括执法主体，执法人员姓名，执法人员所在机构，执法人员电话，执法机构，执法证件号等。	一般 2 级	包含个人基本信息。
	行政处罚公示文书内容	主要包括处罚依据，处罚时间，处罚机关，处罚结果，对处罚事由，案件号，统一信用代码，行政处罚决定书文号，被处罚人名称/姓名，身份证号等。	一般 2 级	包含个人基本信息。
	劳务队伍信息	主要包括上级机构，创建人姓名，劳务队名称，劳务队负责人，手机号码，经营许可证，诚信状况，负责人证件号码等。	一般 2 级	包含个人基本信息。
	来电记录信息	主要包括受理地行政区划代码，受理地行政区划名称，呼叫时间，呼叫流水号，处理人，处理时间，处理结果，处理结果描述，来电号码等。	一般 2 级	包含个人基本信息。
	12328 投诉工单信息	主要包括业务事项，业务事项名称，业务内容，受理地行政区划代码，受理地行政区划名称，受理工号，受理时间，呼入号码，呼叫流水号，呼叫等待时长，处理人，处理时间，处理结果，处理结果描述，工单编号，来电人姓名等。	一般 2 级	包含个人基本信息。

附 录 C
(资料性)
个人信息去标识化脱敏参考示例

个人信息去标识化脱敏措施参考见表C. 1。

表C. 1 个人信息去标识化脱敏措施参考示例

个人信息字段	脱敏措施参考示例
姓名	2个字或3个字的至少隐藏1个字，大于3个字的至少隐藏2个字。示例：×明。
身份证号	显示最后4位，其他隐藏。示例：××××××××××××4136。
证件有效日期和失效日期	显示后4位，其他隐藏。示例：×××0423。
手机号码	显示前3位和后4位，其他隐藏。示例：186××××8937。
邮箱地址	@”前不大于5位的，隐藏前2位；大于5位的，保留前3位，其余隐藏。示例：leyu@163.com脱敏后为××yu@163.com，15890123456@139.com脱敏后为158××××xxxx@139.com。
家庭住址	长度大于12时，只显示前6位，不足12位时，显示不超过50%，其他隐藏。示例：北京市西城区×××××××。
车牌号	保留地区编码和流水号最后2位，其余隐藏。示例：川ANXXX77。
银行卡号	保留前4位和最后4位，中间用×代替。示例：95553301202106561234脱敏后为9555×××××XXX×××1234。
行踪轨迹	直接删除或将其置为NULL值。
照片	采用像素化马赛克处理，将敏感区域分割为色块，降低分辨率（如8×8像素块）。

参 考 文 献

- [1] 中华人民共和国数据安全法
 - [2] 中华人民共和国网络安全法
 - [3] 中华人民共和国个人信息保护法
 - [4] 中华人民共和国密码法
 - [5] 中华人民共和国保守国家秘密法
 - [6] GB/T 25069 信息安全技术 术语
 - [7] GB/T 35274 信息安全技术 大数据服务安全能力要求
 - [8] GB/T 37973 信息安全技术 大数据安全管理指南
 - [9] GB/T 37988 信息安全技术 数据安全能力成熟度模型
 - [10] GB/T 41195 公共信用信息基础数据项规范
 - [11] GB/T 45396 数据安全技术 政务数据处理安全要求
 - [12] JT/T 1480 交通运输数据脱敏指南
 - [13] DB43/T 2845 重要信息系统具体范围和识别规则
 - [14] 《网络数据安全条例》
 - [15] 《公路水路交通运输数据分类分级指南》（交办科技〔2022〕44号）
 - [16] 地理信息数据分类分级工作指南（试行）
-