ICS 35.030
CCS L78

T/CSAS

团　　体　　标　　准

T/CSAS XXXX—2025

轨道交通数据安全要求

Requirements for rail transit data security

（征求意见稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

四川省网络空间安全协会　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。

本文件由四川省网络空间安全协会提出并归口。

本文件起草单位：四川大学，成都墨甲信息科技有限公司，成都信息工程大学，四川中链智网科技有限公司。

本文件主要起草人：

引　言

数字交通作为数字经济发展的重要领域，以数据为关键要素和核心驱动，促进物理和虚拟空间的交通运输活动不断融合和交互。在国务院发布的《“十四五”现代综合交通运输体系发展规划》中，已经明确强调了加强交通运输数据安全的必要性，该规划中提到要完善数据分级分类的安全保护制度，制定智能交通数据应用安全标准，规范数据源的采集、处理和使用，同时加强重要数据与个人信息的保护措施。轨道交通的数字化转型是实现这一目标的重要一环，根据《中国城市轨道交通年度统计报告（2023）》，截至2023年底，中国大陆共有50多个城市开通了轨道交通线路，总运营里程超过7000公里。这一快速扩展带来了巨大的数据流量，而且涉及了包括重要数据与个人信息在内的大量敏感信息，这些信息覆盖了安全运营、商业机密和个人隐私等多个关键领域。因此，确保轨道交通数据安全不仅是提升网络空间安全的战略需求，也是推动交通行业向数字化、智能化发展的基础。为了保障数据在轨道交通领域中的安全性，制定和实施针对性的数据安全标准变得尤为重要。

轨道交通数据安全要求

1 范围

本文件规定了轨道交通数据的安全要求，明确了轨道交通数据安全管理要求、轨道交通数据处理安全技术要求、轨道交通数据风险安全管理要求、轨道交通数据个人信息保护要求、轨道交通数据安全监督要。

本文件规定的轨道交通数据来源于轨道交通系统，包括传统铁路（国家铁路、城际铁路和市域铁路）、城市轨道交通（地铁、轻轨和有轨电车，新型轨道交通有磁悬浮轨道系统、单轨系统）等。

本文件适用于指导轨道交通部门及其技术支撑单位规范轨道交通数据处理和管理活动，也可为监管部门、第三方机构进行监督管理和评估提供参考。

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—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 35274—2023 数据安全技术 大数据服务安全能力要求 术语

GB/T 30012 城市轨道交通运营管理规范

3 术语和定义

下列术语和定义适用于本文件。

GR/T 25069—2022、GR/T 35273—2020和35274—2023界定的以及下列术语和定义适用于本文件。

3.1 数据 data

任何以电子或者其他方式对信息的记录。

[来源：GB/T 43697-2024，3.1]

3.2 数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

[来源：GB/T 35274—2023，3.17]

3.3 数据收集 data collection

根据特定的目的和要求，从一种或多种数据源选择和获取数据，并对数据进行变换、转换、纠错、编码等数据清洗操作，形成数据资产进行存储的数据处理活动。

3.4 数据存储 data storage

将数据持久化保存在硬盘等存储介质中的数据处理活动。

3.5 数据传输 data transmission

数据从一个实体流动到另一个实体的过程。

[来源：GB/T 37988-2019，有修改]

3.6 数据使用 data usage

依据数据权属及收集和使用数据的目的和范围,以及确定的授权和访问控制策略,控制组织、人员或信息系统等主体对数据资产进行读取、检索、展示等操作的数据处理活动。

注： 数据使用需对数据的种类、范围,处理方式及其目的等进行相应的控制,包括数据使用前条件控制和数据使用后义务履行。使用前条件是访问控制引擎在授权过程中,允许主体访问或使用客体数据前需核验的决策因素集。条件控制是用来检查存在的约束限制,数据权属及使用权限是否有效,哪些约束限制需更新等。使用后义务履行是主体在获得对客体的数据使用权限后要执行的要求。主体在获得权限执行数据使用操作后有执行获取这些权限的义务责任。

[来源：GB/T 35274—2023，3.5]

4 轨道交通数据概述

4.1 轨道交通数据定义

轨道交通数据是由轨道交通系统在日常运营、维护和管理过程中生成、传输、存储、处理及分析的所有数据。所述数据具有数据资源量大、更新快、来源多样、结构复杂的特征，具备时空连续性、社会关联性。

4.2 轨道交通数据范围

轨道交通数据包括轨道交通运营数据及个人信息数据，其中，轨道交通运营数据包括：

a) 基础设施数据：涵盖轨道、站台、列车、通信设施、电力供应系统等物理设施的数据。
b) 设备数据：包括列车、信号设备、调度系统、安防监控、应急系统等设备状态和性能数据。
c) 列车运营数据：记录列车运行状态、发车时间、到站时间、班次安排、速度、间隔等与列车调度和运营管理相关的数据。
d) 维护数据：涵盖设备维护、检修、故障处理、保养记录等信息，以保障设备和系统的安全可靠运行。
e) 环境数据：涉及轨道交通沿线的气象、地质、噪声等环境监测数据，以评估和保障外部环境对轨道交通系统的影响。

个人信息数据主要包括：

a) 乘客数据：包括乘客流量、购票信息、乘车记录、投诉反馈等与乘客出行和服务体验相关的数据。
b) 员工数据：包括员工个人信息、考勤和工作记录、健康信息、考勤和工作记录、行为数据、安全与合规记录数据。
c) 供应商与承包商数据：包括身份信息、资质和许可、行为记录数据。

4.3 轨道交通数据形态

轨道交通数据的形态主要包括以下几类：

a) 结构化数据：如时间表、设备维护记录、人员调度表等，可以被数据库或表格系统高效处理的数值型和文本型数据。
b) 非结构化数据：如视频监控数据、图像、声音记录等难以用结构化方式直接存储的数据类型。
c) 半结构化数据：如传感器数据、日志文件等，包含特定格式的标签数据，但不完全符合结构化数据的标准。

5 轨道交通数据安全框架

构建轨道交通数据安全框架的核心目的，是为了系统性地保护轨道交通系统中的各类数据安全，涵盖从运营数据到个人信息的全方位保护。考虑到轨道交通系统的高复杂性和数据的多样性，这一框架需要能够适应数据的实时性、敏感性和多方使用的需求，同时兼顾法律法规的合规性，确保数据的机密性、完整性和可用性。

首先建立数据安全管理要求，从人员和制度方面规定轨道交通数据安全保护的必要行为与措施，确保整个系统中的数据安全工作有章可循。然后对于具体的数据安全防护措施，将轨道交通数据分为“运营数据安全”和“个人信息安全保护”两大技术模块，源于轨道交通数据的多样化特征以及不同数据类别的风险与要求各异。运营数据是轨道交通正常运行的核心，涉及关键业务和流程，因此对其安全保护强调从数据的“全生命周期”出发，确保从数据采集到销毁的每个环节都有明确的安全措施。这样可以有效防范数据泄露、篡改和丢失，保障系统稳定和业务连续性。个人信息数据则聚焦于乘客、员工及相关人员的隐私保护，面临更高的合规性和隐私性要求。因此，在此模块中，框架强调对个人信息主体权利的保障，以及适当的技术手段（如加密、脱敏）的应用，以满足法规要求并提高数据的安全性。

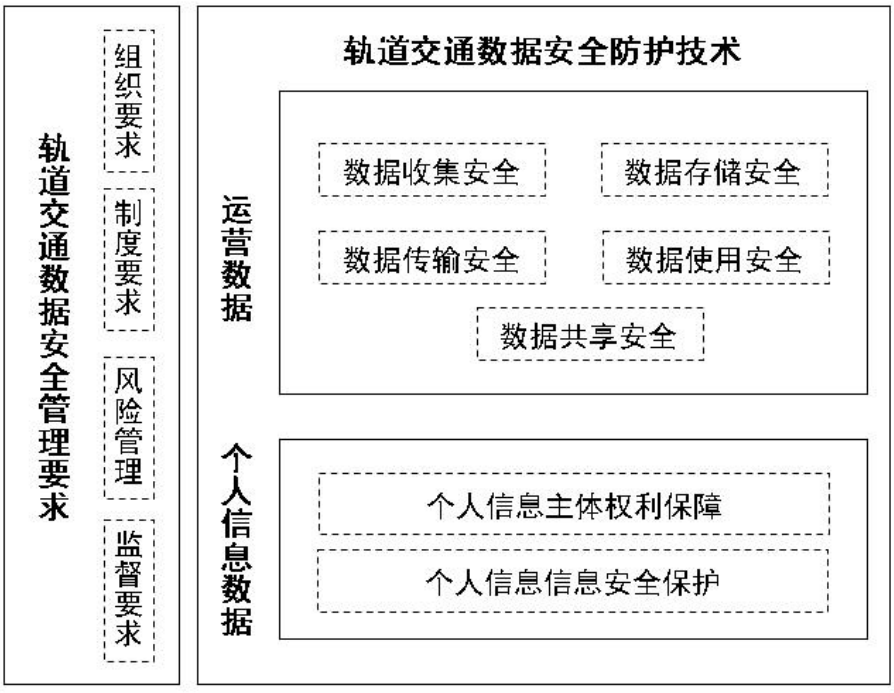

图 1 轨道交通数据安全框架

6 轨道交通数据安全管理要求

6.1 数据安全组织要求

轨道交通数据安全的组织要求主要涉及数据安全的分级和管控，以及相应的数据管理组织机构构建及安全管理规范制定。这些要求旨在确保轨道交通数据的保密性、完整性和可用性，从而保障轨道交通系统的安全运行。

6.1.1 数据安全分级和管控要求

轨道交通数据的安全分级和管控要求规定了不同级别的数据应采取的安全措施和管理策略，以确保数据的安全。这些要求涵盖了数据的分类、存储、传输、使用和处置等方面的安全规定，旨在防止数据泄露、篡改或未经授权的访问。

6.1.2 数据安全管理管理组织

轨道交通数据安全管理组织包括在单位层面建立的数据管理组织和在各业务层级建立的业务数据管理组织，分别负责单位数据治理工作的统筹和各业务数据治理工作的实施。轨道交通数据责任人，通过分层分级原则任命，将数据责任落实到业务主体。数据安全管理组织结构可参考下图所示：

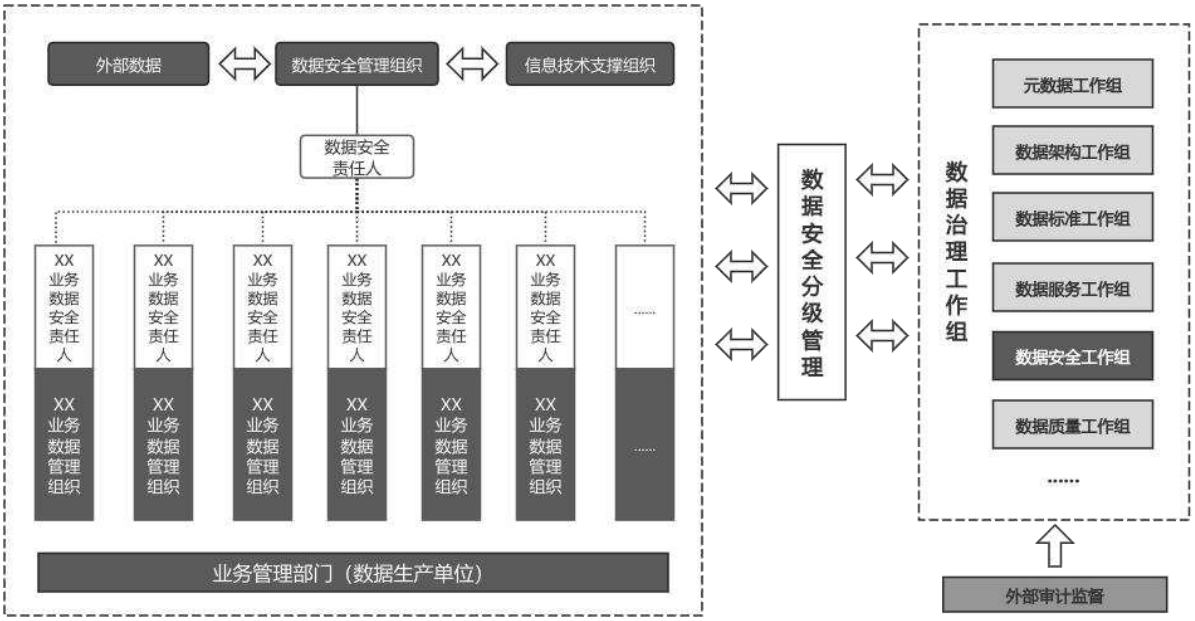

图 2 数据安全管理组织结构

6.1.3 安全管理规范

轨道交通运营安全管理规范详细规定了安全管理的目标、机构设置、全员安全生产责任制、安全管理制度和操作规程、安全生产投入等方面的要求。这些规范确保了轨道交通系统的安全运行，包括但不限于车辆、通信、信号系统的安全，以及应急处理和救援措施的有效性。

6.2 数据安全制度要求

加强轨道交通数据信息安全保护，确保轨道交通运输安全、稳定、高效运行，依据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等相关法律法规，结合轨道交通行业实际，制定适用于轨道交通企业内部涉及数据信息管理的各个环节，包括数据采集、存储、传输、处理、使用、共享、销毁等。

轨道交通数据安全制度要求主要包括数据安全分级和数据管控要求，旨在确保轨道交通领域的数据安全。这些要求由中华人民共和国交通运输部发布，旨在保护关键信息基础设施的安全，维护网络安全。具体要求如下：

6.2.1 数据管控制度

规定了数据的收集、存储、处理、传输和处置等方面的具体管理措施，以确保数据的安全性和隐私保护。轨道交通数据信息安全管理工作应遵循以下原则：

a) 依法合规：严格遵守国家法律法规，确保数据信息安全；
b) 安全优先：将数据信息安全放在首位，确保轨道交通运输安全；
c) 分级管理：根据数据信息的重要性、敏感程度和影响范围，实施分级保护；
d) 责任明确：明确数据信息安全责任，落实岗位责任制；
e) 持续改进：不断优化数据信息安全管理制度，提高数据信息安全保障能力。

6.2.2 数据安全分类分级制度

根据数据的敏感程度和重要性，对轨道交通数据进行分类，以确保不同级别的数据得到相应的保护措施。

（一）轨道交通数据信息安全分为以下类别：

a) 基础数据：包括轨道交通基础设施、设备、运输组织、运营管理等基础信息；
b) 业务数据：包括旅客、货物运输、客运服务、财务管理等业务信息；
c) 技术数据：包括轨道交通通信、信号、控制系统等技术信息；
d) 其他数据：包括员工信息、企业内部管理等其他信息。

（二）轨道交通数据信息安全分为以下等级：

a) 一级数据：对轨道交通运输安全、稳定、高效运行具有决定性影响的敏感数据；
b) 二级数据：对轨道交通运输安全、稳定、高效运行具有重要影响的敏感数据；
c) 三级数据：对轨道交通运输安全、稳定、高效运行有一定影响的敏感数据；
d) 普通数据：对轨道交通运输安全、稳定、高效运行影响较小或不影响的数据。

6.3 数据风险安全管理要求

数据风险安全管理要求主要包括以下几个方面：

a) 明确数据安全政策：首先，需要制定明确的数据安全政策，明确数据的所有权、使用权限和保密责任。政策应涵盖数据的收集、存储、处理、使用和传输等方面，明确员工和第三方合作伙伴在数据安全方面的职责；
b) 建立数据安全组织结构：设立专门的数据安全管理团队，并为其提供足够的权力和资源。这个团队应负责监督政策的执行、提供技术支持、管理风险，并在发生安全事件时协调应对。同时，应在各部门之间建立跨部门的数据安全协作机制，以确保数据安全的全面覆盖；
c) 运用先进的数据安全技术：加强网络安全措施，如使用强大的防火墙和入侵检测系统来防止未经授权的访问。重视数据加密和访问控制，以防止数据泄露和非法访问。利用数据备份和恢复技术，确保在发生安全事件时能迅速恢复正常运营；

d) 制定并执行应急响应计划：对于可能发生的各种数据安全威胁，应制定应急响应计划，包括事前预防、事中响应和事后恢复的全过程。定期进行安全审计和风险评估，及时发现和修复潜在的安全漏洞；

e) 进行数据安全风险评估：随着信息技术的发展，组织内部的数据规模和复杂性不断增加，这意味着数据安全风险也在不断上升。数据安全风险评估是识别并管理此类风险的关键步骤。通过评估，可以确定潜在的安全漏洞，预测可能发生的数据泄露或其他安全事件，并采取预防措施来降低或消除这些风险。

6.4 数据安全监督要求

轨道交通数据安全监督要求主要包括遵守法律法规、尊重社会公德和伦理、遵守商业道德和职业道德、诚实守信、履行数据安全保护义务、承担社会责任，以及不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

在针对轨道交通数据安全管控监督等制度时要充分考虑相关法律法规的要求，如《网络安全法》等，这些法规明确规定了组织在数据安全管理中的责任和义务，确保数据的安全。组织必须遵守所在地的相关法规，保障数据的完整性、保密性和可用性等。包括引入权威第三方监测机构的部门协作机制，加大对监测数据弄虚作假行为的查处力度等，以促进形成一批专业化、优质化的社会监测机构。

7 轨道交通数据处理安全技术要求

7.1 运营数据安全技术要求

7.1.1 数据收集

轨道交通运营数据采集阶段是通过对数据采集过程进行合法合规的过程管理，对采集设备及数据源的可靠性、安全性进行有效的防护。数据采集的安全措施要包括以下内容：

a) 定义数据采集的目的和用途，明确数据源和采集范围；

b) 遵循合法正当原则，确保数据采集符合轨道交通运营管理的合法性、规范性、正当性和必要性，不进行跨权限的数据采集；

c) 对采集的数据信分类分级标识，并对不同级别的数据实施相应的安全管理策略和保障措施；

d) 制定采集数据的清洗、转换、加载等操作规范，明确操作方法、手段，并做好备份工作，避免操作过程中出现数据遗漏、丢失等问题。

e) 轨道交通数据采集分级安全措施应包括下列内容 ：

f) 采集2级及以上数据时，应跟踪和记录采集过程 ，并采取技术措施确保所收集信息来源可追溯，具备条件的单位宜记录1级及以上数据的信息来源 ；

g) 从单位外部系统采集 3 级及以上数据时， 应结合口令密码、设备物理位置、网络接入方式 、设备风险情况等多种因素对数据采集设备或系统的安全性进行增强验证; APP、WEB等客户端完成采集后不应留存3级及以上数据, 并及时清理缓存；

h) 从单位外部系统采集4级及以上数据时 ，应对采集的数据进行加密 ，对采集全过程进行持续动态认证, 确保数据采集设备或系统的真实性, 必要时可实施阻断、二次认证等操作。

7.1.2 数据存储

轨道交通数据存储阶段的主要数据安全目标是防止存储数据的泄露和未授权的修改 、删除和销毁。数据存储一般安全措施应包括下列内容：