7117ICS 35.040
L80

CIIA

中 国 信 息 协 会 团 体 标 准

T/CIIA XXX—2023

智慧城市数据安全技术框架

Smart city data security technical framework

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国信息协会发布

目 录

前　言

本标准按照GB/T1.1-2020《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。
本标准由中国信息协会提出并归口。
本标准由中国信息协会信用专业委员会提出。
本标准起草单位：XXX、XXX、XXX、XXX、XXX、XXX
本标准主要起草人：XXX、XXX、XXX、XXX、XXX、XXX

智慧城市数据安全技术框架

1 范围

本标准提出了智慧城市数据安全技术框架，包括智慧城市数据安全管理保障、智慧城市数据安全技术保障以及智慧城市数据安全运营保障等。

本标准适用于为智慧城市数据安全保障能力的规划、管理、建设及运营提供参考。

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 25069-2010 信息安全技术 术语

GB/T 37043-2018 智慧城市 术语

GB/T 34678-2017 智慧城市 技术参考模型

GB/T 37971-2019 信息安全技术 智慧城市安全体系框架

GB_T 37973-2019 信息安全技术 大数据安全管理指南

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 39477-2020 信息安全技术 政务信息共享 数据安全技术要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

3 术语和定义

3.1 智慧城市 smart city

运用信息通信技术，有效整合各类城市管理系统，实现城市各系统间信息资源共享和业务协同，推动城市管理和服务智慧化，提升城市运行管理和公共服务水平，提高城市居民幸福感和满意度，实现可持续发展的一种创新型城市。

[来源：GB/T 37043-2018 智慧城市 术语，2.1.1]

3.2 数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[来源：GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型 术语，3.1]

3.3 数据活动 data activity

数据的收集、存储、加工、使用、提供、交易、公开等行为。

3.4 时空数据 spatiotemporal data

本文件中的时空数据是指以城市为对象，基于统一时空基准的，与位置直接或间接相关联的地理要素或现象信息的数据。

4 缩略语

下列缩略语适用于本文件

ICT 信息通信技术 （information communication technology）

5 智慧城市数据安全概述

5.1 智慧城市数据活动

智慧城市数据活动主要是数据作为生产要素在不同处理者之间进行交换、处理的动作。根据智慧城市ICT体系的物联感知层、网络通信层、计算与存储层、数据及服务融合层、智慧应用层的特点，智慧城市数据活动情况如下图所示。

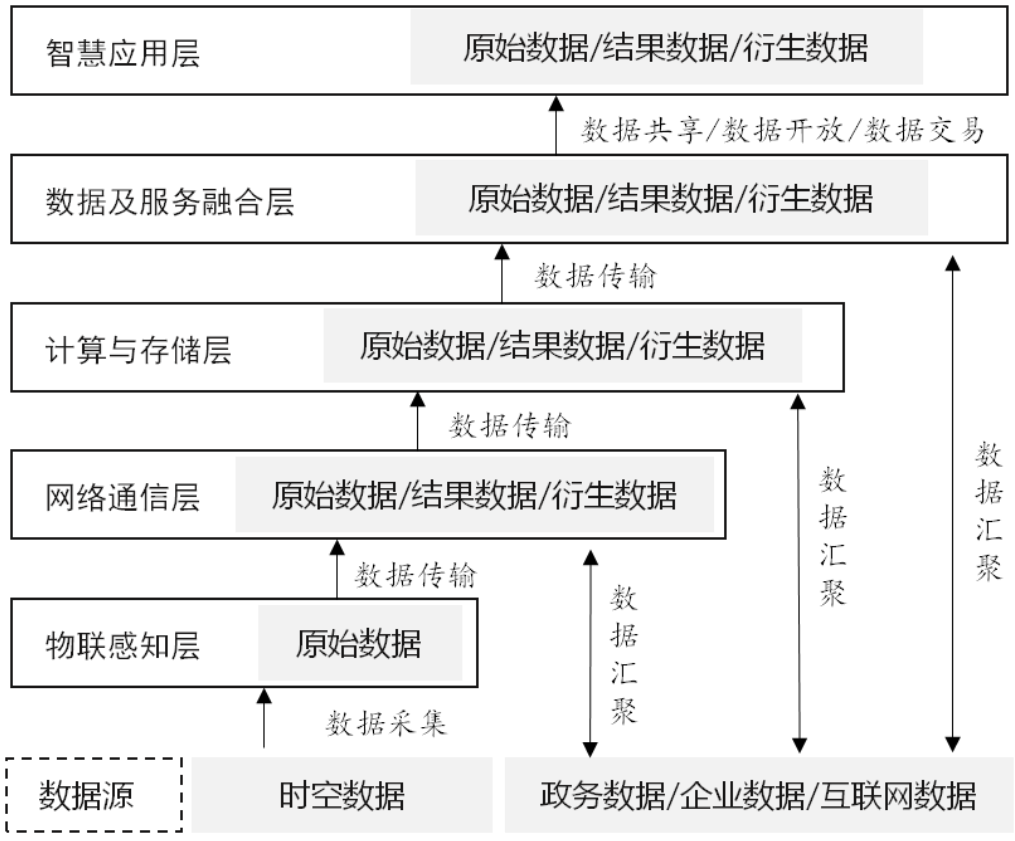

图1 智慧城市数据活动示意

5.2 智慧城市数据安全保护需求

智慧城市数据安全保护需求基于数据活动所处的环境关注数据的真实性、完整性和可用性，以支撑智慧城市多源数据的共享、开放与流通为目标，通过管理手段、技术手段、运营保障相结合，形成系统的数据安全保障体系，全面防范安全风险，保证智慧城市数据相关业务安全稳定运行。

6 智慧城市数据安全技术框架概述

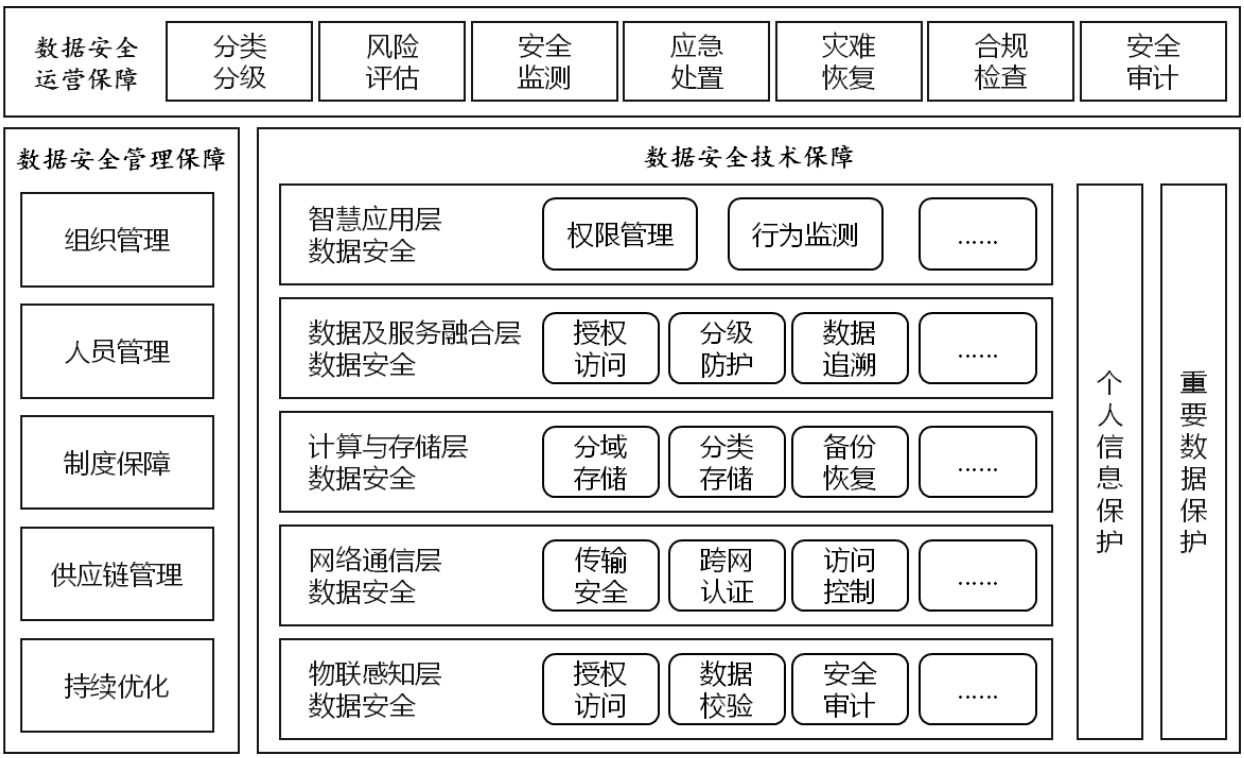

图2　智慧城市数据安全技术框架

智慧城市数据安全技术框架由数据安全管理保障、数据安全技术保障以及数据安全运营保障组成。

其中，数据安全管理保障是通过制度流程设计优化、组织人员管理及其他措施从管理层面保障数据安全的能力。包括组织管理、人员管理、制度保障、供应链管理和评价优化。

数据安全技术保障从智慧城市数据处理的架构出发，围绕数据处理收集、存储、使用、加工、传输、提供、公开等环节，规范每个层级中对数据的安全保护技术措施。包括物联感知层数据安全、网络通信层数据安全、计算与存储层数据安全、数据及服务融合层数据安全、智慧应用层数据安全等。对于个人信息和重要数据的安全要求贯穿其中。

数据安全运营保障通过建立常态化的技术、管理流程的系统工程，以保障业务正常运转过程中数据资产的安全。包括分类分级、风险评估、安全监测、应急处置、合规检查以及安全审计等。

7　智慧城市数据安全管理保障

7.1　组织管理

本项要求包括：

a)　具备数据安全管理相关机构，指定组织最高管理者或授权代表担任负责人，组织内承担数据安全的责任人和从事数据安全保护人员为成员，明确各岗位的职责和权限。

b)　明确数据安全管理机构的常设部门和专职部门，负责沟通协调组织内外协作事宜和执行数据安全组织的日常工作。

c)　形成数据安全沟通机制，由相关机构适时组织实施数据安全通报、政策研讨、发展规划决策，以及数据安全工作奖惩等。

7.2　人员管理

本项要求包括：

a) 明确内部员工、临时人员或外部协作人员等的职责分工、安全责任和数据处理权限范围等。
b) 数据安全管理机构应与人事部门协商制定员工入职和离职的安全审查流程和机制，签署或确认相关人员的保密协议书。
c) 建立重要数据或核心数据处理备案机制，常态化管理涉重要数据和核心数据处理人员，排查数据泄露或数据滥用风险并及时采取防范措施。
d) 建立常态化的数据安全意识教育和安全保护技能培训机制，整体提升人员数据安全能力。

7.3 制度保障

本项要求包括：

a) 制定总体的数据安全方针策略和数据安全管理办法，设定管理原则和职责分工，以及系统安全管理、数据安全管理、用户使用安全管理、安全监测与事件应急处置和监督考核等。
b) 制定数据分类分级实施规范、个人信息保护实施规范，数据跨境保护规范等，明确保护目标、管理要求、职责分工和实施流程等。
c) 制定数据管理规范、人员管理规范和数据安全事件管理规范等，明确保护目标、管理要求、职责分工和实施流程等。

7.4 供应链管理

本项要求包括：

a) 建立供应链数据安全风险管理制度，明确安全责任人和安全管理机构，组织实施供应链数据安全风险处置工作，研究解决重大风险问题。
b) 对供应商提出数据安全相关能力要求，通过认证认可、评价等形式保证供应商数据安全能力。
c) 组织推动供应链数据安全能力建设，定期开展数据安全监测和风险评估工作，收集与供应链数据安全相关的信息，及时采取风险防范措施。

7.5 持续优化

本项要求包括：

a) 建立数据安全持续改进优化机制，基于当前数据安全合规性和执行效果进行评估，不断进行优化和迭代。
b) 执行效果评估包括但不限于以下项目，评估数据汇集、数据传输、数据存储、数据加工、数据开放共享、数据删除与销毁等操作合规性和技术措施所处水平。评估数据安全管理和运营保障能力，主要包括数据安全组织和人员设置，管理制度、安全监测、运维与应急响应能力等的执行效果。

8 智慧城市数据安全技术保障

8.1 物联感知层数据安全

本项要求包括：

a) 制定数据采集规范，对采集数据进行校验，实施采集的业务系统中应具备必要的访问授权机制；
b) 建立数据采集日志，实现对数据采集过程的可追溯；
c) 明确数据存储和数据清除的有效期，在有效期后进行相应处理；
d) 存在计算场景的，对计算后的数据状态进行审计和评估，确保数据完整性、可用性。

8.2 网络通信层数据安全

本项要求包括：

a) 采取安全通道、可信通道、数据加密等安全控制措施保障数据传输安全；
b) 支持对传输数据完整性的检查，根据数据分级分类定义，对相应类型和级别数据配备相应数据完整性校验手段，发现数据传输过程中的丢失或损坏，并具备相应的恢复控制措施；
c) 对跨域网络通信首先进行跨域认证，并对跨域网络传输进行加密。
d) 在关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制，应在关键网络节点处监视网络攻击行为。

8.3 计算与存储层数据安全

本项要求包括：

a) 根据不同的数据类型、数据容量、业务需求建立相应的数据存储逻辑，根据数据重要性、量级、使用频率等因素，将数据分类分域存储，明确数据存储隔离规则和授权管理机制；
b) 设置存储和备份策略和操作规程，如自动备份、数据保护、数据校验等策略；
c) 对数据存储进行审计，对数据存储过程的身份鉴别、策略管理、备份作业、恢复作业等操作，以及管理员和用户的各类操作进行安全审计；
d) 对访问数据存储系统的各类行为进行访问控制，对各种异常访问行为进行监测和处置；
e) 采用符合国家相关标准规定的数据加密方式与密码算法；
f) 采用技术手段对网络出口的数据进行检测，识别定义的敏感数据，阻断传输行为，防止对外泄漏；
g) 加强存储介质存储内容和使用权限管理，对介质访问和使用行为进行记录和审计；
h) 制定数据的备份策略和恢复策略，包括本地备份和异地备份等方式；
i) 建立针对数据内容和存储介质的数据清除和销毁的机制，包括数据销毁策略和管理制度、数据销毁审批机制，明确销毁方式和销毁要求。

8.4 数据及服务融合层数据安全

本项要求包括：

a) 数据处理应提供相应的鉴权机制，按数据分类分级结果对各类数据设置访问策略、传播策略和传播范围等；
b) 对处理的原始数据进行敏感度识别，防止重要数据或核心数据非授权处理，并对处理过程中产生的敏感数据应进行脱敏；
c) 对数据处理过程中的数据操作行为进行日志记录，以备对分析结果质量和真实性进行溯源；
d) 建立共享数据审核机制，明确数据共享范围、共享方式、共享内容，根据不同级别数据制定不同的共享策略和数据的安全要求，防止越权共享数据；
e) 对数据共享接收方提出安全要求，确保其具有相应的数据安全防护能力，保障共享数据安全；
f) 对数据共享使用 API 的接口传输、授权、监控等环节建立安全防护措施，对 API 接口数据交换内容进行识别和管控；
g) 在数据共享过程中采用内容识别、多方安全计算、可信执行环境、联邦学习、同态加密、差分隐私等技术，保障共享数据的隐私性、正确性、完整性；
h) 在数据共享过程中采用标签、指纹、水印等技术进行溯源管理，保障数据共享过程的可追溯性。

8.5 智慧应用层数据安全

本项要求包括：

a） 对应用数据、应用数据相关活动进行备案，根据参与方角色，配置相应权限；

b） 对应用层数据及操作行为进行监测、信息采集、记录和分析，并对应用数据监测结果进行风险分析。

8.6 个人信息保护

本项要求包括：

a） 智慧城市数据使用者作为个人信息控制者，收集、存储、使用个人信息等活动应满足 GB/T 35273-2020 对个人信息安全的要求；

b） 个人信息应分类分级，个人生物识别信息、个人实名身份信息应与其他个人信息分离存储；

c） 个人信息存储、处理、委托处理、共享、转让、公开披露时，应采用足够强度的去标识化技术、访问控制技术进行保护；

d） 传输和存储敏感个人信息时，应采用加密等安全措施；对超过 100 万条个人信息的加密，应遵循国家密码管理相关标准，采用符合国产商用密码的技术和产品；

e） 对收集个人敏感信息、开展自动化决策等活动前，应进行个人信息安全影响评估。

8.7 重要数据保护

本项要求包括：

a） 参照重要数据识别相关标准，对智慧城市重要数据进行识别，并形成重要数据目录清单；

b） 参照重要数据处理相关标准，对重要数据全生命周期安全进行针对性保护。

9 智慧城市数据安全运营保障

9.1 分类分级

本项要求包括：

a） 建立数据资产管理系统，扫描、登记、管理智慧城市数据资产，形成数据资产清单；

b） 参照相关标准，建立智慧城市分类和分级规则，形成数据分类分级清单，并生成数字化标识；

c） 在数据保护要求、目标和法律法规发生变化时，持续优化分类分级规则和方法。

9.2 风险评估

本项要求包括：

a） 定期开展重要数据及敏感个人信息数据的安全评估，识别数据资产价值，识别数据资产的脆弱性及安全威胁，客观评定数据安全风险等级，形成数据安全风险评估报告；

b） 及时整改数据安全评估中发现的风险隐患和问题，完善数据安全保护措施；

c） 在新业务上线前、重要数据出境、开放共享前，以及涉及第三方管理等场景中，应进行数据安全动态评估，形成数据安全风险评估报告，明确整改措施并严格执行。

9.3 安全监测

本项要求包括：

a） 结合数据分类分级标签对重要数据、敏感个人信息数据的数据访问行为、数据权限变化、数据流程变化、数据暴露面等的情况进行实时监测；

b） 及时将监测到的漏洞隐患或安全事件按照要求进行通报、下发、预警提醒，对通报情况和处理情况进行统计、分析、展示和提供不同类型的总结报告。

9.4 应急处置

本项要求包括：

a) 制定应急响应制度，明确数据安全事件管理部门和配合部门、数据安全事件发现及报告机制、应急保障措施、追踪溯源及处置流程、事件跟踪总结等；
b) 根据业务场景制定应急预案，配套相关措施，并根据应急预案，制定演练计划并定期组织演练，保存演练记录；
c) 在发生数据安全事件时及时按照应急响应制度和应急预案实施应急措施。

9.5 灾难恢复

本项要求包括：

a) 具备数据安全事件灾难恢复策略与预案；
b) 具备数据安全事件灾难恢复资源，包括但不限于数据备份、备用数据处理系统等。

9.6 合规检查

本项要求包括：

a) 跟根据法律法规以及标准规范的要求，形成智慧城市数据安全合规要求知识库并持续更新；
b) 组建团队并形成数据安全检查标准化执行机制和检查实施处理的制度和流程；
c) 建立数据安全检查相关平台，配置安全管理策略，支撑日常数据安全检查；
d) 建立进行数据安全检查所需的相关工具，包括但不限于资产识别工具、审计工具、操作管理工具、行为分析工具等；
e) 建立数据安全检查结果处理监督机制，根据数据安全检查结果、整改计划等对执行情况进行监督。

9.7 安全审计

本项要求包括：

a) 建立数据安全审计机制，明确审计目的、审计对象、审计操作规程、审计频度、审计结果规范等内容；
b) 明确数据安全审计工作涉及部门和人员的权限和责任，并明确相关权限的授予规程；
c) 明确数据安全审计的内容，包括但不限于内部权限控制、内部数据流向跟踪情况、数据安全保障措施有效性等；
d) 组织内部或外部审计团队开展数据安全审计，记录并形成数据安全审计报告，针对有关问题提出改进方案，并要求落实解决，对改进措施落实情况进行跟踪审核。