

T/CUPC

团 体 标 准

T/CUPC 0**—2026

人工智能赋能智慧城市建设通用技术要求 与实施指南

General Technical Requirements and Implementation Guidelines for AI-Empowered
Smart City Construction

**** – ** – **发布

**** – ** – **实施

目 次

前 言	I
引 言	I
1 范围	2
2 规范性引用文件	2
3 术语和定义	2
4 缩略语	3
5 总体原则	4
6 参考架构	4
7 通用技术要求	6
8 实施指南	8
9 安全保障与伦理治理	10
10 评价与持续改进	11
附 录 A （资料性） 场景类型	12
附 录 B （资料性） 评价指标	13
附 录 C （资料性） 城市 AI 能力成熟度评估模型	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。

本文件由*****等单位提出，由中国城镇化促进会归口。

本文件主要起草单位：*****

本文件参与起草单位：*****

本文件主要起草人：*****

引言

当前，人工智能技术正以前所未有的速度融入城市发展的各个领域，成为推动城市治理体系和治理能力现代化的重要引擎。随着大模型、智能体、具身智能等前沿技术的快速演进，城市正在从“数据驱动”向“模型智能”范式转变，人工智能赋能智慧城市建设（以下简称“城市 AI”）已成为全球城市数字化转型的主流方向。

然而，城市 AI 建设仍面临一系列挑战：一是缺乏统一的参考架构和通用技术要求，各地建设模式差异大，重复建设和“数据孤岛”问题突出；二是城市大模型、AI 智能体等新技术的部署缺乏规范性指引，模型安全、算法治理和伦理风险防控机制尚不健全；三是场景选择和实施路径缺乏科学依据，试点经验难以规模化推广；四是评价体系不完善，难以量化城市 AI 建设成效并指导持续改进。

在此背景下，制定本文件具有重要的现实意义：

本文件明确了城市 AI 的术语定义、参考架构和通用技术要求，为城市开展 AI 赋能智慧城市建设的规划、设计、实施、运营和评估提供系统性指引，促进各地建设实践的规范化与标准化。

本文件在 GB/T 45402—2025 城市智能中枢参考架构基础上，强化了 AI 能力层的独立性和核心地位，将城市大模型、AI 智能体和 MLOps 纳入标准能力支撑范畴，推动城市 AI 从零散应用向平台化、体系化方向发展。

本文件系统规定了数据安全、模型安全、算法治理和伦理准则要求，建立了覆盖 AI 系统全生命周期的安全保障与伦理治理框架，为城市 AI 的可信、可控、可持续发展提供制度保障。

本文件提出了“规划—试点—推广—优化”四阶段实施路径和智能体自主性分级管理机制，引导城市结合实际、因地制宜、循序渐进地推进城市 AI 建设，实现技术创新与风险防控的动态平衡。

本文件建立了涵盖基础设施、数据治理、模型能力、应用效果、安全合规和市民满意度等维度的评价指标体系和能力成熟度评估模型，为城市 AI 建设的成效评估和持续优化提供科学依据。

人工智能赋能智慧城市建设通用技术要求与实施指南

1 范围

本文件规定了人工智能赋能智慧城市建设（城市AI）的总体原则、参考架构、通用技术要求、实施指南、安全保障与伦理治理、评价与持续改进等内容。

本文件适用于指导城市开展人工智能赋能智慧城市建设（城市AI）的规划、设计、实施、运营和评估工作，也可作为相关技术产品和服务的研发、测试与选型提供参考。

注：本文件适用于地级及以上城市，县级市、城市区（县）可参照执行。

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 35273 个人信息安全规范

GB/T 37988 数据安全能力成熟度模型

GB/T 34678—2017 智慧城市 技术参考模型

GB/T 36333—2018 智慧城市 顶层设计指南

GB/T 37043—2018 智慧城市 术语

GB/T 42888-2023 信息安全技术 机器学习算法安全评估规范

GB/T 43441.1—2023 信息技术 数字孪生 第1部分：通用要求

GB/T 43697-2024 数据安全技术 数据分类分级规则

GB/T 45081-2024 人工智能 管理体系

GB/T 45402—2025 智慧城市 城市智能中枢 参考架构

GB/T 45288.1-2025 人工智能 大模型 第1部分：通用要求

GB 45438-2025 网络安全技术 人工智能生成合成内容标识方法

GB/T 45654-2025 网络安全技术 生成式人工智能服务安全基本要求

GB/Z 185.1-2026 人工智能 智能体互联 第1部分：总体架构

ISO 37106:2021 Sustainable cities and communities — Guidance on establishing smart city operating models for sustainable communities

ISO/IEC 24039:2022 Information technology — Smart city digital platform — Reference architecture

3 术语和定义

GB/T 37043—2018和GB/T 45402—2025界定的以及下列术语和定义适用于本文件。

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，推动城市管理和公共服务智慧化，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。

[GB/T 37043—2018，定义2.1.1]

3.2

人工智能赋能智慧城市（城市 AI） AI-empowered smart city

以人工智能为核心驱动力，通过对城市多源数据的智能感知、认知推理和决策优化，实现城市运行管理、公共服务、产业发展的智能化升级，推动城市从“数据驱动”向“模型智能”范式转变的城市发展形态。

3.3

城市智能中枢 city intelligent center

综合应用新一代信息技术，融合城市多源数据资源，整合状态感知、建模分析、城市运行管理、应急指挥等功能，通过人机交互与协同，提供态势全面感知、趋势智能研判、协同高效处置、调度敏捷响应、平急快速切换等智能化服务，提升城市精准精细治理水平，支撑城市数字化转型的一种复杂系统。

3.4

大模型 large-scale model

大规模深度学习模型 large-scale deep learning model

基于大量数据训练得到，具有复杂计算架构，能处理复杂任务，且具备一定泛化性的深度学习模型。注：大模型的参数量由其功能和模态决定，一般不低于1亿。大模型训练使用的数据总量受参数量的影响，达到收敛的大模型的参数量的对数与其训练数据总量的对数成正比。

[GB/T 45288.1-2025，定义3.1]

3.5

城市大模型 urban large-scale model

基于大模型等人工智能技术构建，具备自主感知、推理决策、工具调用和任务执行能力的软件实体，在城市业务场景下应接受人类监督，关键节点接受人工干预，协同完成复杂任务。

3.6

智能体 agent

感知环境，并主动采取行动以实现特定目标的实体。

[GB/Z 185.1-2026，定义3.1]

3.7

具身智能系统 embodied intelligence system

基于物理实体进行感知、行动的智能系统（简称具身智能），其通过物理交互获取信息、理解问题、做出规划并实现行动，从而实现智能增长和行动自适应。

3.8

数字孪生 digital twin

具有保证物理状态和虚拟状态之间以适当速率和精度同步的数据连接的特定目标实体的数字化表达。

[GB/T43441.1—2023，定义3.4]

3.9

数字孪生城市 digital twin city

通过多源数据融合和模型构建，在数字空间中建立与物理城市实时映射、动态交互的虚拟城市系统，为AI推理和决策提供仿真验证环境。

3.10

算法治理 algorithmic governance

对城市AI系统中使用的算法进行登记、评估、监测和优化的制度与技术安排，旨在确保算法的公平性、透明性和可问责性。

4 缩略语

下列缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）

LLM：大语言模型（Large Language Model）

MLOps：机器学习运维（Machine Learning Operations）

RAG：检索增强生成（Retrieval-Augmented Generation）

API：应用程序编程接口（Application Programming Interface）

SLA：服务水平协议（Service Level Agreement）

GPU：图形处理器（Graphics Processing Unit）

NPU：神经网络处理器（Neural Processing Unit）

TPU：张量处理器（Tensor Processing Unit）

SDK：软件开发工具包（Software Development Kit）

5 总体原则

5.1 以人为本原则

- a) AI技术的部署应以提升市民福祉、保障公共利益为根本目标。
- b) 应确保AI服务的包容性和可及性，避免算法歧视，关注老年人、残障人士、低收入群体等特殊需求。
- c) 市民参与应贯穿AI系统设计、部署和评估全过程。

5.2 统分结合原则

- a) 应坚持“城市统建、部门分用”原则。
- b) 城市层面统一建设AI基础设施、城市大模型、智能体和智能中枢，各部门基于统一底座开发行业应用，避免重复建设和“数据孤岛”。

5.3 安全可控原则

- a) AI系统的训练、部署和运行应符合国家数据安全和网络安全法律法规。
- b) 关键AI系统应实现自主可控，模型训练数据应来源合法、质量可靠，算法决策应可解释、可审计。

5.4 开放兼容原则

- a) AI平台应遵循开放技术标准和接口规范，支持多厂商、多技术路线兼容。
- b) 应避免技术锁定，保障城市对AI基础设施和核心能力的持续掌控。

5.5 迭代演进原则

- a) AI赋能智慧城市建设（城市AI）是持续演进的过程。
- b) 应采用“小步快跑、迭代优化”的实施策略，建立AI系统持续学习和模型更新的长效机制。

6 参考架构

6.1 总体架构

人工智能赋能智慧城市（城市AI）的参考架构以城市智能中枢为核心，自底向上分为基础设施层、数据资源层、AI能力层、能力开放层、智慧应用层，并辅以安全保障和运维运营两大支撑体系。具体如下图：



图 1 参考架构

注：该架构在GB/T 45402—2025 城市智能中枢总体架构基础上，强化了AI能力层的独立性和核心地位，将城市大模型、AI智能体和MLOps纳入标准能力支撑范畴。

6.2 各层要求

6.2.1 基础设施层

- 宜提供AI训练和推理所需的异构算力资源（GPU、NPU等），支持算力弹性调度和按需分配。
- 宜具备支持大规模模型训练的高速存储和网络能力。
- 物联网感知设施宜按需支持AI边缘推理，具备本地数据预处理能力。

6.2.2 数据资源层

- 应建立面向AI训练的城市数据治理体系，包括数据采集、清洗、标注、脱敏和版本管理。
- 应构建城市知识库和知识图谱，为城市大模型提供检索增强生成（RAG）的知识底座。
- 数据资源应支持多模态（文本、图像、视频、时空数据）统一存储和检索。
- 应明确数据持有、加工使用、经营权归属，遵循“原始数据不出域、可用不可见”原则，涉及个人信息的须依法授权并去标识化，确保来源合法、使用可追溯可审计。

6.2.3 AI 能力层

AI能力层是赋能智慧城市的核心层级，应包括但不限于：

- 城市大模型：基于城市领域数据训练或微调的大规模基础模型，具备城市运行规律理解、跨领域推理和自然语言交互能力；
- AI智能体平台：支持智能体的编排、调度和执行，提供工具调用、多步推理和任务规划能力；
- 视觉与多模态分析引擎：提供城市视频分析、图像识别、遥感解译等视觉智能能力；
- 预测与优化引擎：提供交通流预测、能耗优化、风险预警等预测性分析能力；
- MLOps平台：支撑模型的训练、评估、部署、监控和持续迭代。

6.2.4 能力开放层

- 应以API、SDK、微服务等形式向各部门和外部开发者开放AI能力。

- b) 应提供统一的能力目录、调用计量和配额管理机制。应支持低代码/无代码的AI应用开发方式，降低AI使用门槛。

6.2.5 智慧应用层

- a) 应面向城市治理、民生服务、产业经济、生态宜居等领域提供AI增强的应用服务。
- b) 应用开发应遵循“大模型+知识库”范式，通过提示工程和智能体编排实现业务逻辑。

6.2.6 安全保障与运维运营

- a) 安全保障体系应覆盖AI系统的全生命周期，包括模型安全、数据安全、应用安全和基础设施安全。
- b) 运维运营体系应建立AI系统的日常监控、性能优化和事件响应机制。

7 通用技术要求

7.1 城市大模型技术要求

7.1.1 模型能力

城市大模型应具备以下核心能力：

- a) 城市知识理解：能够准确理解和回答关于城市运行、政策法规、公共服务等领域的问题；
- b) 跨领域推理：能够综合交通、气象、人口、经济等多领域信息进行关联推理；
- c) 多模态处理：支持文本、图像、视频、时空数据的联合理解和分析；
- d) 工具调用：能够通过API调用外部工具和服务完成复杂任务；
- e) 持续学习：支持基于新数据的增量学习与知识更新，避免灾难性遗忘，具备知识盲区识别、版本管理与溯源能力，并满足幻觉率、事实性准确率、拒绝回答边界等可靠性量化要求。

7.1.2 模型训练与微调

- a) 训练数据应来源于城市政务数据、公共服务数据、互联网公开数据等合法渠道，应经过脱敏和合规审查；
- b) 应建立训练数据的质量评估和偏见检测机制；
- c) 微调应针对城市特定场景和知识领域进行，确保模型输出符合城市治理规范；
- d) 模型版本应统一管理，支持回滚和灰度发布。

7.1.3 模型部署

- a) 支持云端集中部署和边缘分布式部署两种模式；
- b) 推理服务应满足城市关键业务的时延要求，关键场景响应时间宜控制在秒级以内；
- c) 应具备模型服务的弹性扩缩容能力，适应业务负载波动；
- d) 应支持模型量化、蒸馏等轻量化技术，降低部署成本。

7.2 城市 AI 智能体技术要求

7.2.1 城市 AI 智能体架构

- a) 城市AI智能体应由感知模块、推理引擎、工具集、记忆模块和执行器组成。
- b) 推理引擎应支持多步规划和任务分解，工具集应提供城市业务系统的标准化调用接口。

7.2.2 多智能体协同

- a) 应支持多个城市AI智能体之间的任务分配、信息共享和协同执行；
- b) 应建立智能体通信协议和协调机制，避免资源冲突和任务重复；
- c) 应支持人类监督和干预机制，关键决策节点应保留人工确认环节。

7.2.3 自主性分级

城市AI智能体的自主性应分级管理，如下表：

表1 分级管理

级别	自主程度	适用场景	监督要求
L1	辅助建议	决策支持、信息检索	人工决策
L2	人机协同	工单分派、异常检测	人工确认关键节点
L3	条件自主	信号优化、资源调度	人工监督、异常干预
L4	高度自主	常规巡检、数据更新、事后设计	设置异常阈值，一旦触发异常自动触发人工介入

7.3 数据治理技术要求

7.3.1 数据质量

- a) 应建立城市数据质量评估指标体系，包括完整性、准确性、一致性、时效性等维度；
- b) 训练数据应经过清洗、去重、标注和校验，标注质量应达到场景要求；
- c) 应建立数据溯源机制，记录数据来源、处理过程和版本变更。

7.3.2 数据安全和隐私

- a) 训练数据中的个人信息应经过脱敏处理，符合《个人信息保护法》要求；
- b) 宜支持联邦学习、差分隐私等隐私增强技术；
- c) 敏感数据的访问应实行最小权限原则和全流程审计。

7.3.3 知识库构建

- a) 应构建城市领域知识库，涵盖政策法规、业务流程、地理信息、历史案例等；
- b) 知识库应支持结构化查询和语义检索；
- c) 知识库更新应与政策变化和业务调整保持同步。

7.4 算力基础设施要求

7.4.1 算力资源

- a) 应根据城市AI应用需求，配置适当的异构算力资源（GPU/NPU/TPU）；
- b) 算力资源应支持池化管理、动态调度和弹性分配；
- c) 应支持训练算力和推理算力的分离部署和按需调配。

7.4.2 算力网络

- a) 应构建支持算力互联的网络架构，实现多数据中心之间的算力协同；
- b) 应支持算力资源的统一纳管和跨域调度；

- c) 边缘算力节点应满足低时延AI推理需求。

7.5 应用开发技术要求

7.5.1 开发范式

AI增强的城市应用开发，应采用“大模型+知识库+智能体”的开发范式：

- a) 以城市大模型为通用认知能力底座；
- b) 以城市知识库为领域知识来源，通过RAG技术增强模型输出的准确性和时效性；
- c) 以城市AI智能体为任务执行单元，通过编排和协同完成复杂业务流程。

7.5.2 提示工程

- a) 应建立提示模板库，规范各类城市场景的提示设计；
- b) 关键应用的提示应经过测试和优化，确保输出质量和稳定性；
- c) 应建立提示版本管理和效果评估机制。

7.5.3 人机交互

- a) 应提供自然语言交互入口，降低用户使用门槛；
- b) 关键决策场景应提供可解释性输出，说明AI建议的依据和置信度；
- c) 应支持多轮对话和上下文理解，提升交互体验。

8 实施指南

8.1 实施路径

AI赋能智慧城市（城市AI）建设宜采用“规划—试点—推广—优化”四阶段实施路径。

8.1.1 规划阶段

主要任务，包括但不限于：

- a) 评估城市AI的基础设施现状和业务需求；
- b) 制定AI赋能智慧城市顶层设计，明确建设目标、重点场景和实施计划；
- c) 建立组织保障机制，明确牵头部门和协同机制；
- d) 开展数据资源盘点和治理规划。

8.1.2 试点阶段

主要任务，包括但不限于：

- a) 建设城市大模型和AI能力平台的最小可用版本；
- b) 选择2-3个高价值场景开展试点（如智能工单分派、交通信号优化、政务服务问答），试点应包括风险评估，优先选择风险等级中低的场景开展试点，高风险城市AI场景不宜作为首批试点；
- c) 建立MLOps流程和模型评估机制；
- d) 积累运营经验，形成可复制的实施模板。

8.1.3 推广阶段

主要任务，包括但不限于：

- a) 将试点成果向更多部门和场景推广；
- b) 完善城市AI能力开放平台，支持多部门自主开发AI应用；

- c) 建立城市AI应用效果评估和反馈机制；
- d) 培养城市AI人才队伍。

8.1.4 优化阶段

主要任务，包括但不限于：

- a) 持续优化城市大模型和知识库；
- b) 扩展城市AI智能体应用范围，提升自主性级别；
- c) 建立城市AI系统性能监控和持续改进机制；
- d) 跟踪城市AI技术发展，适时引入新技术和新方法。

8.2 组织保障

8.2.1 领导机制

- a) 宜成立AI赋能智慧城市（城市AI）建设工作领导小组，由政府主要领导或分管领导担任组长，统筹协调各部门工作。
- b) 领导小组办公室宜设在城市数据管理部门或智慧城市主管部门。

8.2.2 部门协同

- a) 数据管理部门负责数据资源统筹和AI平台建设；
- b) 各业务部门负责本领域AI应用的需求定义和场景落地；
- c) 信息化部门负责技术标准和接口规范的统一；
- d) 应建立跨部门的城市AI应用评审和协调机制。

8.2.3 人才队伍

- a) 应建立城市AI的人才梯队，包括算法工程师、数据工程师、AI产品经理和业务专家；
- b) 宜设立“城市AI的职能专业人员”岗位，承担技术与公共政策之间的桥梁角色；
- c) 应定期开展城市AI的素养培训，提升全员AI应用能力。

8.3 场景选择与优先级

8.3.1 场景选择原则

- a) 高价值：对城市治理或公共服务有显著提升效果；
- b) 数据就绪：具备可用的数据资源；
- c) 技术可行：现有AI技术能够支撑；
- d) 风险可控：AI决策的影响范围可管理；
- e) 可衡量：效果可通过量化指标评估。

8.3.2 优先场景建议

见附录A。

8.4 供应商管理

- a) 应建立城市AI 供应商准入标准和评估机制，关注技术能力、数据安全和服务可持续性；
- b) 关键城市AI 基础设施（城市大模型、算力平台）应优先选择自主可控的技术方案；
- c) 应避免对单一供应商的过度依赖，核心能力和数据资产应保留在城市侧；
- d) 合同应明确数据所有权、模型知识产权和退出机制，当采用第三方公有云大模型服务时，应明确城市业务数据不得用于第三方模型训练。

9 安全保障与伦理治理

9.1 数据安全

- a) 城市 AI 的数据安全应遵循 GB/T 35273、GB/T 37988 等数据安全标准；
- b) 城市 AI 的系统应按 GB/T 22239 落实网络等级保护要求；
- c) 涉及关键信息基础设施的，应符合 GB/T 39024 的要求；
- d) 训练数据的采集、存储、使用和销毁应全流程合规；
- e) 应按 GB/T 43697 的要求，建立数据分类分级保护制度，敏感数据应加密存储和传输；
- f) 跨境数据传输应符合国家法律法规要求。

9.2 模型安全

- g) 城市 AI 的模型安全应遵循 GB 45438-2025、GB/T 45654-2025、GB/T 45081-2024、GB/T 42888-2023 等模型安全标准；
- h) 应建立模型安全评估机制，检测模型的后门、偏见和鲁棒性问题；
- i) 模型输出应经过内容安全过滤，防止有害信息生成；
- j) 应建立模型对抗攻击的防御机制；
- k) 关键模型应定期进行安全审计和红队测试；
- l) 应按规定履行生成式人工智能服务备案、安全评估等手续；
- m) 城市 AI 应用若对外输出生成内容（政务问答、宣传素材、视频分析报告等）必须落实显示/隐式标识。

9.3 算法治理

- a) 应建立城市 AI 算法登记制度，记录算法用途、数据来源、决策逻辑和风险等级，符合国家算法备案要求的，可与其衔接；
- b) 高风险算法（影响公民权益、公共安全等）应进行算法影响评估；
- c) 应确保算法决策的可解释性，关键场景应能说明决策依据；
- d) 应建立算法投诉和救济渠道。

9.4 伦理准则

- a) 公平性：AI 系统应避免对特定群体的歧视，定期检测和纠正算法偏见；
- b) 透明性：AI 决策应可追溯、可解释，市民有权了解影响自身权益的 AI 决策逻辑；
- c) 可问责性：应明确 AI 系统错误决策的责任主体和追责机制；
- d) 人类监督：涉及公民重大权益的城市 AI 决策应保留人工审核环节；
- e) 包容性：AI 服务应覆盖不同群体，避免加剧数字鸿沟。

9.5 风险管理

宜参照《人工智能安全治理框架》最新版的内容，建立城市 AI 风险管理的“映射—测量—管理—治理”闭环：

- a) 映射：识别 AI 系统在城市场景中的风险来源和影响范围；
- b) 测量：建立风险评估指标，量化风险等级；
- c) 管理：制定风险应对措施，包括规避、减轻、转移和接受；
- d) 治理：建立风险管理的组织机制和制度保障。

注1：风险包括三类，内生风险（模型幻觉、算法偏见、数据投毒、算力供应链断供）、应用风险（智能体越权失控、具身智能物理伤害、信息内容违规、个人信息侵害）、衍生风险（就业冲击、伦理失范、城市关键设施受扰）；

注2：按应用场景重要性、智能化水平、应用规范，风险划分为严重、高、中、低；

注3：明确研发者、提供者、使用者三方责任；实行模型版本回退、漏洞追溯、定期审计；沙箱监管设定退出条件等。

10 评价与持续改进

10.1 评价指标体系

AI赋能智慧城市建设（城市AI）的评价宜从基础设施、数据治理、模型能力、应用效果、安全合规、市民满意度维度开展，具体见附录C。

10.2 评价方法

- a) 宜采用定量与定性相结合的评价方法，数据来源于系统监测、用户反馈和第三方评估；
- b) 宜建立城市AI能力成熟度评估模型（参见附录C），定期评估城市AI发展水平；
- c) 评价结果应作为城市AI系统优化和资源配置的重要依据。

10.3 持续改进

- a) 应建立城市AI系统性能的常态化监控机制，及时发现和解决性能退化问题；
- b) 应建立用户反馈收集和处理机制，将用户需求纳入迭代计划；
- c) 应跟踪城市AI技术发展趋势，适时引入新技术和新方法；
- d) 应定期开展城市AI应用效果复盘，总结经验并优化实施方案。

附 录 A
(资料性)
场景类型

表A 场景类型

优先级	场景类型	典型应用	预期效果
高	智能工单分派	城市管理事件自动分类与派单等	效率提升 40%以上
高	政务智能问答	政策咨询、办事指南等	减少人工客服 60%
高	视频智能分析	占道经营、暴露垃圾识别等	发现效率提升 20%以上
中	交通信号优化	自适应配时、绿波带等	通行效率提升 15%
中	能耗优化	建筑节能、路灯调光等	能耗降低 10%—15%
中	风险预警	内涝、火灾、人群聚集等	预警提前量提升

附 录 B
(资料性)
评价指标

表B 评价指标

B. 1城市AI评价指标

维度	关键指标	目标值建议
基础设施	算力资源利用率、AI 服务可用性	利用率≥60%，可用性 ≥99.9%
数据治理	训练数据质量达标率、数据更新时效	达标率≥95%
模型能力	城市大模型问答准确率、推理响应时间	准确率≥85%，响应≤3 秒
应用效果	AI 应用覆盖率、业务流程效率提升	覆盖率逐年提升
安全合规	安全事件数量、算法登记率	重大事件为 0，登记率 100%
市民满意度	AI 服务使用率、市民评价	满意度≥80%

附 录 C

(资料性)

城市 AI 能力成熟度评估模型

C.1 城市 AI 成熟度等级

等级	名称	特征描述
L1	初始级	零散 AI 应用，无统一平台和数据治理
L2	规范级	建立 AI 平台和数据治理体系，应用场景有限
L3	集成级	AI 能力与业务流程深度融合，多场景覆盖
L4	智能级	城市大模型驱动，AI 智能体协同，自适应优化
L5	引领级	全域数智化，持续创新，成为城市核心竞争力

C.2 评估维度与权重

评估维度	权重	关键评估项
基础设施	15%	算力规模、弹性调度、边缘能力
数据治理	20%	数据质量、知识库建设、安全合规
模型能力	25%	大模型性能、多模态、持续学习
应用深度	25%	场景覆盖、流程融合、自主性级别
治理体系	15%	算法登记、伦理审查、风险管理

参考文献

- [1] 国家信息中心，华为云. AI CITY发展研究报告——“人工智能+”时代的发展范式创新[R]. 2025.
- [2] ISO 37127-2 城市和社区可持续发展 智慧城市运营模型中的人工智能应用 第2部分：原则与要素（立项中）.
- [3] NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0) [S]. 2023.
- [4] 《人工智能安全治理框架3.0》.