

TC609

全国数据标准化技术委员会技术文件

TC609-4-2026-07

城市全域数字化转型 城市智能体应用建设 指引

City-wide digital transformation — Construction guidance of the city intelligent
agent applications

2026-10-23 发布

2026-10-23 实施

全国数据标准化技术委员会 发布

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 缩略语	2
5 基本原则	2
6 城市智能体能力	3
6.1 基本概述	3
6.2 感知智能	3
6.2.1 感知设备	3
6.2.2 数据传输	3
6.3 认知智能	4
6.3.1 语料库与知识库	4
6.3.2 深度理解	4
6.3.3 智能推理	4
6.4 执行智能	4
6.4.1 自主决策	4
6.4.2 任务规划	5
6.4.3 任务调度与执行	5
6.4.4 结果评估与优化	5
6.5 服务智能	6
6.5.1 智能体编排	6
6.5.2 智能体网关	6
6.5.3 智能体观测	6
6.5.4 会话记忆	6
6.5.5 智能体资产管理	6
6.5.6 开发过程支持	7
7 城市智能体典型应用场景描述	7
7.1 城市治理	7
7.2 惠民服务	7
7.3 数字经济	8
7.4 城市更新	8
8 城市智能体建设路径	9
8.1 场景识别	9
8.1.1 场景分析	9
8.1.2 数据需求分析	10

- 8.2 打造高质量数据集 12
- 8.3 构建 AI 能力 12
 - 8.3.1 概述 12
 - 8.3.2 基础 AI 能力建设 12
 - 8.3.3 大模型训练与优化 12
 - 8.3.4 知识库与语料库构建 13
- 8.4 搭建智能体 14
 - 8.4.1 AI 能力封装与服务化 14
 - 8.4.2 AI 能力安全与合规 15
 - 8.4.3 AI 能力评估与认证 16
 - 8.4.4 智能体协同 17
- 8.5 智能体运营 18
 - 8.5.1 安全运营 18
 - 8.5.2 资产运营 18
 - 8.5.3 业务价值运营 19
 - 8.5.4 运行维护 19
 - 8.5.5 智能体管理 19
 - 8.5.6 智能体退役 20
- 参 考 文 献 21

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。

本文件由全国数据标准化技术委员会（SAC/TC609）提出并归口。

本文件起草单位：重庆信息通信研究院、北京思特奇信息技术股份有限公司、中国电子技术标准化研究院、数族科技（南京）股份有限公司、安阳数智科技集团有限公司、浙江省质量科学研究院、数融智联（徐州）信息科技有限公司、联想（北京）有限公司、广州智能科技有限公司、联通数据智能有限公司、北京新瑞锦世数智科技有限公司、大连深方信息科技有限公司、国家数据发展研究院、中移雄安信息通信科技有限公司、杭州高新区（滨江）区块链与数据安全研究院、华为技术有限公司、建筑材料工业信息中心、南京理工大学、深圳开鸿数字产业发展有限公司、广州维视达数字科技有限公司、山东未来集团有限公司、中国人民大学、南威软件股份有限公司、浪潮智慧城市科技有限公司、扬州市大数据管理中心、重庆市大数据应用发展管理局、重庆市数字化城市运行和治理中心、武汉云计算科技有限公司、北京建筑大学、山西远大纵横科技有限公司、深圳市有方科技股份有限公司、嘉兴市文诺财经大数据技术研究院、中国质量认证中心有限公司、中电信数政科技有限公司、联通（江苏）产业互联网有限公司、中电信数智科技有限公司、北京兴云数科技术有限公司、北京优锆科技股份有限公司。

城市全域数字化转型 城市智能体应用建设指引

1 范围

本文件给出了城市智能体应用建设的基本原则、能力要求和典型应用场景，确立了城市智能体应用的建设路径。

本文件适用于城市智能体应用的规划设计、建设与运营。

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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 43697-2024 数据安全技术 数据分类分级规则

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/T 46347-2025 人工智能 风险管理能力评估

TC609-5-2025-1 高质量数据集 建设指南

TC609-4-2026-01 城市全域数字化转型 城市感知体系建设导则

3 术语和定义

下列术语和定义适用于本文件。

3.1

城市全域数字化转型 **city-wide digital transformation**

城市以全面深化数据融通和开发利用为主线，综合利用数字技术和制度创新工具，实现技术架构重塑、城市管理流程变革和产城深度融合，促进城市发展全领域增效、支撑能力全方位增强、转型生态全过程优化的城市高质量发展新模式。

3.2

高质量数据集 **high-quality dataset**

经过采集、加工等数据处理，可直接用于开发和训练人工智能模型，能有效提升模型性能及泛化能力的数据集合。

[来源：TC609-5-2025-1，3.2，有修改]

3.3

智能体 **intelligent agent**

能够感知环境并利用工具采取行动以实现特定目标的系统。

注：智能体以大模型为智能底座，具备自主感知、理解、规划、决策、记忆、行动的能力，能够自动化执行复杂任务，具有自主性、交互性、反应性和适应性等基本特征。

[来源：ISO/IEC 22989:2023，3.1.1，有修改]

3.4

大模型 large-scale 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。

[来源：GB/T 45288.1—2025，3.1]

4 缩略语

下列缩略语适用于本文件。

AI：人工智能(Artificial Intelligence)

API：应用编程接口(Application Programming Interface)

GIS：地理信息系统(Geographic Information System)

SLA：服务水平协议(Service Level Agreement)

CIM：城市信息模型(City Information Modeling)

BIM：建筑信息模型(Building Information Modeling)

MCP：模型上下文协议(Model Context Protocol)

A2A：智能体交互协议(Agent-to-Agent)

ANP：智能体通信协议(Agent Network Protocol)

AHP：层次分析法(Analytic Hierarchy Process)

GPU：图形处理器(Graphics Processing Unit)

TPU：强量处理单元(Tensor Processing Unit)

HTTPS：超文本传输安全协议(Hypertext Transfer Protocol Secure)

5 基本原则

城市智能体应用建设的基本原则包括：

- a) 统筹规划，系统协同。强化城市智能体全域一体化布局，坚持共建共享、集约高效利用原则，统筹算力、算法、数据、感知设施等核心资源，杜绝重复投入与资源浪费，实现横向跨领域协同、纵向上下级贯通，推动多智能体高效联动、协同发力；
- b) 以人为本，需求导向。以提升市民获得感、幸福感、安全感为根本出发点，坚持场景驱动、需求引领，应用城市智能体提升就业、医疗、教育等便民惠民服务精准度与普惠性；
- c) 数据驱动，数智赋能。深度整合政务、交通、能源、环境、民生等多领域数据资源，构建覆盖城市全要素、全周期的高质量数据集；通过人工智能、大数据分析、知识图谱等技术手段，对海量数据进行深度挖掘与智能分析，通过智能体实现对城市运行状态的精准洞察、趋势预测和智能决策支持；
- d) 安全可控，可信可靠。构建城市智能体安全体系，落实数据分类分级、权限管控、脱敏处理，筑牢数据安全与系统运行安全防线，切实保障公民隐私权益与数据合法使用，确保城市智能体稳定有序运行；
- e) 开放合作，协同共建。构建政府引导、企业主导、社会参与的智能体协同共建机制，政府负责规划、标准、监管与公共场景供给；企业主导建设、运营与技术创新；社会力量广泛参与，激

发多元主体活力，推动政产学研用深度融合，整合跨领域资源，打造开放共享、互利共赢的城市智能体生态；

- f) 伦理向善，公平问责。伦理向善贯穿城市智能体全生命周期，恪守公平、透明、可解释、可问责四大准则。杜绝算法偏见，保障决策无歧视；公开关键逻辑，维护公众知情权；明确责任主体，定期开展伦理审查与风险评估，持续迭代优化，确保城市智能体始终锚定公共利益。

6 城市智能体能力要求

6.1 基本概述

城市智能体具备感知、认知、执行、服务等核心能力，实现对城市运行状态的全面感知、深度理解、智能推理、自主决策规划、精准执行与持续优化。分别描述如下：

- a) 感知智能：通过部署在城市各处的多源异构感知设备，实现对城市人、物、空间、过程的实时数据采集、传输，构建城市智能体的数据基础；
- b) 认知智能：通过数据治理形成高质量的语料库与知识库，并利用自然语言理解、视觉理解、多模态理解以及逻辑推理与模型推理等技术，实现对城市运行状态的智能分析、趋势预测与决策支持，为执行提供可解释、可追溯的依据；
- c) 执行智能：能将认知阶段产生的结果转化为对城市实体设备、业务流程或服务系统的具体操作，支持跨系统、跨智能体的协同执行与闭环控制；
- d) 服务智能：面向政府、企业、市民等用户，提供统一的智能体服务接口与能力开放平台，并配套安全合规要求，保障城市智能体服务的可控、可信与合规。

6.2 感知智能

6.2.1 感知设备

感知设备能力要求包括：

- a) 多维采集能力：具备视频、音频、物联传感、射频识别及空间定位等多模态数据的采集能力，采集政务数据、个人信息等敏感数据需完成合规授权流程，公开采集数据需提前公示范围与用途，支持对城市部件、人员、车辆、事件及环境参数的精准识别与监测；
- b) 边端处理能力：感知终端宜具备边缘计算能力，支持在源端进行数据清洗、特征提取、隐私脱敏及实时分析；
- c) 控制交互能力：感知终端具备可配置的控制接口，支持响应上层指令，实现对末端设备的远程控制、自动调节及状态校准；
- d) 感知终端符合 TC609-4-2026-01 中 6.1 的要求。

6.2.2 数据传输

数据传输能力要求包括：

- a) 泛在网络接入：具备异构网络融合接入能力，包括但不限于以太网、光纤接入（PON）、4G/5G/6G/NB-IoT、高低轨卫星通信、无线自组网、新一代 WLAN 及星闪等，符合 TC609-4-2026-01 中 6.2 的要求；
- b) 数据接入：支持主流的数据格式，具备统一的设备标识与注册机制；
- c) 数据流通安全可信：支持基于数据分类分级要求或信息系统安全等级要求，提供对应等级的数据可信流通服务，确保数据在网络中流通的安全可信；

- d) 高并发与高性能：满足城市级高密度连接需求，并为关键业务提供微秒级时延与确定性带宽保障（SLA）；
- e) 内生安全：建立设备入网的实时鉴权与信任机制，具备防范非法终端接入、数据加密传输及异常流量清洗的能力，确保链路安全可信。

6.3 认知智能

6.3.1 语料库与知识库

语料库与知识库建设应符合TC609-5-2025-1要求，城市智能体需要的语料库与知识库包括：

- a) 城市治理基础语料库：面向城市管理的动态数据汇聚中心，聚焦政务服务、城市交通、环境、安防等领域的实时与历史数据，支撑政务智能问答自动审批、交通拥堵预警、环境质量监测、公共安全事件识别等核心场景；
- b) 部门知识库：政府各职能部门内部的专业化知识管理系统，聚焦部门业务规则、审批流程、历史决策等结构化知识的沉淀与应用，提升跨部门协作效率。功能包括知识结构化录入、版本控制、跨部门知识协同，以及基于业务场景的知识智能推送；
- c) 公共知识库：面向社会公众开放的知识服务平台，汇聚法律法规、公共服务信息、城市基础数据等普惠性知识资源。通过城市智能体问答功能解答市民办事疑问，促进公共知识的普及与传播，提升城市服务的可及性与透明度。

6.3.2 深度理解

深度理解能力使城市智能体能够从多源异构数据中提取语义信息，是认知智能的核心入口。深度理解能力要求包括：

- a) 自然语言理解：支持多轮对话、多语言的语义解析、情感识别，进行意图和社会行为分析；
- b) 视觉理解：支持目标检测、行为识别、事件理解；
- c) 上下文理解：具备处理长篇文档和复杂文本的能力，支持上下文关联理解和跨段落信息整合；
- d) 多模态理解：支持同时处理图像、文本、语音、传感器数据等多种模态信息，实现模态间的语义对齐与互补增强；
- e) 跨模态理解：图文匹配、视频与文本联合理解。

6.3.3 智能推理

智能推理能力基于理解后的信息进行逻辑推导与模型计算，为规划与决策提供可信结论。智能推理能力要求包括：

- a) 逻辑推理：支持规则推理、案例推理与图推理（如知识图谱推理）；基于规则或数据进行演绎、归纳、溯因推理；基于不完全信息进行不确定性推理，输出带置信度的结论；
- b) 模型推理：支持在线实时推理与离线批量推理，具备多种主流模型格式的统一部署与服务化能力。通过资源动态调度与请求队列管理，保障高并发、大数据量场景下的低延迟与高可用。

6.4 执行智能

6.4.1 自主决策

自主决策能力基于认知智能的分析结果，结合实时数据与历史经验，生成可执行的决策方案。自主决策能力要求包括：

- a) 支持基于实时数据与历史经验的智能决策，支持人机协同决策；
- b) 支持决策解释机制，提供可追溯的决策依据；

- c) 支持策略仿真预演与效果量化评估，自动推荐最优预案并支持多预案对比；
- d) 在进行推理决策时，需先检索相关知识库/法规库，确保输出的准确性和合规性，防止大模型幻觉导致的错误决策。

6.4.2 任务规划

任务规划能力将决策目标分解为可执行的任务序列，明确任务依赖与约束条件，生成结构化的执行计划。任务规划能力要求包括：

- a) 自主分解任务并生成执行步骤；
- b) 支持多目标优化与约束满足，输出可执行方案序列；
- c) 支持将自然语言或结构化决策指令解析为原子任务与复合任务；
- d) 具备任务依赖关系分析，生成有向无环图（DAG）执行计划；
- e) 支持对时间、资源、权限等约束条件的识别与绑定。

6.4.3 任务调度与执行

任务调度与执行能力负责将规划结果落地为实际控制指令。任务调度与执行能力要求包括：

- a) 任务调度：
 - 1) 支持原子/复合任务的排序与并行调度；
 - 2) 具备优先级抢占与资源冲突消解能力，保障关键任务优先执行；
- b) 工具调用：
 - 1) 支持工具的注册、发现与调用；
 - 2) 工具调用接口需认证、加密、鉴权；
- c) 模型协同：支持模型协同推理与执行；
- d) 多智能体协同：
 - 1) 支持各类多智能体协作模式，包含主席智能体和执行智能体的经典模式；
 - 2) 支持基于 A2A 等标准协议框架；
 - 3) 支持智能体之间使用符合标准的通信协议（如 MCP、A2A、ANP 及扩展其他协议）进行通信和交互；
- e) 执行保障：
 - 1) 建立严格的“最小权限原则”与“独立沙箱隔离”机制。执行进程运行于独立容器沙箱，文件系统只读；采用最小权限原则，每个任务仅授予所需 API 的最小集合；所有输出指令须经过静态规则白名单校验；
 - 2) 端到端执行时延满足城市实时场景要求，支持毫秒级设备控制指令下发；
 - 3) 实时监控执行状态，支持任务重试、回滚或转移，确保高可用性；
 - 4) 支持在执行过程中动态感知环境变化，包括网络延迟、设备离线、计算资源过载、突发事件等；
 - 5) 在不中断整体任务的前提下，自动调整剩余任务拆解方案与资源分配；
 - 6) 支持基于实时反馈的策略热更新（无需重启服务）。

6.4.4 结果评估与优化

结果评估与优化能力要求包括：

- a) 每个原子任务执行完成后，反馈执行结果；
- b) 应能检测执行偏差，并触发自动补偿或重试机制；

- c) 完整记录执行日志包括含时间戳、输入输出、中间状态、最终结果、异常堆栈等，日志保存期限不少于 1 年，用于事后审计、问题溯源与模型优化；
- a) 能够从历史执行结果中积累经验，识别重复出现的城市运行模式，形成可复用的知识库；
- b) 具有模型持续迭代与版本管理机制，基于反馈数据持续优化决策策略，动态更新知识图谱与规则库，保持认知能力的时效性与准确性。

6.5 服务智能

6.5.1 智能体编排

支持可视化拖拽式或者基于代码的工作流设计，允许开发者通过流程方式定义智能体的思考路径、任务拆解逻辑和决策分支，实现复杂城市业务逻辑的自动化处理。

6.5.2 智能体网关

智能体接入网关在保证处理所有流入流量的前提下，确保安全、可靠和高可用。智能体网关要求包括：

- a) 统一的 API 入口，负责请求路由、组合和协议转换；
- b) 统一处理身份认证、权限鉴定、访问限流和请求日志；
- c) 提供智能体运行地址注册，用于智能体路由。

6.5.3 智能体观测

可观测性是监控和理解智能体生态系统端到端行为的过程，包括智能体与大语言模型和外部工具进行的任何交互。智能体观测要求包括：

- a) 实时汇聚智能体的各种运行数据，包含智能体访问的知识、各类工具、大模型、提示词、推理决策等信息；
- b) 制定智能体服务的核心观测指标，包含性能、可用性、准确性、响应延迟等。对日志进行智能分析，及时识别大模型的处理性能瓶颈、效率损耗和可靠性风险等问题。同时将日志数据实时同步至安全中心，支撑智能体的实时安全监控与动态防护；
- c) 提供智能体运行可视化看板，展现智能体运行核心指标。

6.5.4 会话记忆

会话记忆是指在多轮交互中保持上下文信息的能力，用于提升服务的连续性与个性化。会话记忆要求包括：

- a) 支持会话的短期、中期和长期记忆。明确不同时长记忆的存储期限与定期清理机制，不同的记忆可以采用不同的存储系统；
- b) 支持会话的摘要存储，提升会话的存储效率和使用效率；
- c) 支持会话敏感信息的脱敏、加密等措施，提升存储安全。

6.5.5 智能体资产管理

智能体资产管理是对城市范围内各级智能体进行注册、发布、查询与全生命周期管控的机制。智能体资产管理要求包括：

- a) 用于城市范围内不同级别的智能体资产管控，包含城市级、行业级、企业级等；
- b) 支持智能体的注册和发布。注册的智能体应是经过评测后的安全智能体；
- c) 可以被查询和订阅。

6.5.6 开发过程支持

开发过程支持是为智能体建设提供工具链与环境支撑的能力，能力要求包括：

- a) 支持各类相关资产的注册和使用，包含提示词、工具等；
- b) 支持智能体的调试、评估、发布等。

7 城市智能体典型应用场景描述

7.1 城市治理

城市治理以构建多元共治格局为导向，通过城市智能体提升精准决策、预警应急与精细化治理能力，部分应用举例见表1。

表 1 城市智能体在城市治理场景应用举例

序号	应用场景	场景描述
1	全域感知智能体	集成摄像头、烟感、智能井盖等物联网设备，实时解析视频与传感器信号，识别高空抛物、消防通道占压、燃气泄漏等风险事件。根据风险等级生成工单推送至网格员终端，联动门禁与广播系统执行管控。结合 BIM、人口热力、车辆轨迹等数据构建社区数字孪生，通过强化学习优化停车位调度、垃圾清运路径等资源分配
2	政务服务智能体	建立统一资源目录，实现企业基本信息、信用、社保等数据的归集、脱敏与共享。自动解析营业执照、身份证明等材料，通过规则引擎完成真实性核验、合规性审查与地址比对，实现材料自动审核
3	政务办公智能体	集成语音识别与声纹认证，实时转写会议音频为结构化文本，提取议题、观点与结论，生成带任务清单的会议纪要。基于政策法规知识图谱，辅助输出符合格式要求的公文初稿。自动拆决议事项为任务，匹配责任部门与责任人，推送督办提醒并生成执行进度看板
4	城市运行智能体	汇聚政务、交通、环境、卫健等数据，构建城市数据湖。基于 CIM 数字孪生平台，推演交通拥堵、空气污染、疫情传播等模式，生成警力部署、信号灯配时、公交接驳、污染源管控、封控区划定等预案。跨部门联动系统将预案拆解为任务，同步推送至交管、环保、卫健、城管等部门执行
5	环境治理智能体	集成卫星遥感、无人机影像及地面微站数据，对 PM2.5、COD、土壤重金属进行时空配准，构建生态环境数字孪生，定位污染传输路径与风险区划。部署视频行为识别算法，自动检测垃圾混投并触发语音提醒。运用强化学习优化收运路径，结合气象与污染溯源模型预警重污染天气，推送至相关部门协同处置
6	城市更新与建筑安全智能体	整合住建、应急、消防及物业的建筑数据，构建建筑数字档案。利用 BIM/CIM 平台对老旧建筑进行安全风险动态评级与可视化展示。对更新方案进行日照、能耗、交通等多维度模拟比选；通过物联网与 BIM 模型比对，实现重大修缮工程的非现场监管
7	基层治理智能体	整合社区人口、房屋、巡查记录与居民反馈，对接政务系统，识别矛盾风险点并预警。分析民生诉求热点，监测异常事件（安全隐患、群体事件苗头），实现任务调度、协同处置与决策支持

7.2 惠民服务

以提升居民生活品质为目标，通过城市智能体优化公共服务资源配置，增强医疗、教育、文化等领域的智能化服务水平，实现便捷、普惠、个性化的数字生活体验，部分应用举例见表2。

表 2 城市智能体在惠民服务场景应用举例

序号	应用场景	场景描述
1	医疗服务智能体	对接 120 急救、医院信息系统、医院 HIS、居民电子健康档案及可穿戴设备，构建医疗数据湖。急救场景下，综合位置、路况、医院饱和度、生命体征，动态生成最优路径、最近可用医院及绿色通道方案。慢病管理场景下，通过隐私保护的联合训练构建疾病风险预测模型，生成个性化干预建议推送至家庭医生。持续追踪结果数据反哺模型迭代
2	教育资源智能体	汇聚教师资质、课程信息、学生画像等数据，构建“师-生-课-场”数字孪生。将时间、容量、设备、志愿等约束转化为目标函数，生成最优课表。课后服务中，基于兴趣标签与资源池构建双边匹配模型，生成个性化服务清单。追踪课程效果与满意度，动态调整资源配置
3	公共文化智能体	运用客流热力图与聚类分析识别博物馆拥堵节点，通过强化学习优化展品布局与参观路径；图书馆场景中自动识别热门书籍并触发补货预警，结合室内定位提供 AR 导航。针对大型活动，导入 BIM 与人群行为参数，仿真疏散过程，自动生成撤离路线、警力部署、医疗救援等预案。实时监测人流密度，超阈值时触发广播引导与闸机限流

7.3 数字经济

数字经济以推动产业数字化转型为核心，通过城市智能体赋能制造业、农业、电商、文化资源等领域，促进数据要素流通与资源配置优化，培育新质生产力，助力经济高质量发展，部分应用举例见表3。

表 3 城市智能体在数字经济场景应用举例

序号	应用场景	场景描述
1	文化资源智能体	运用激光扫描、倾斜摄影与光谱成像，对文物与古建筑进行全要素数字化采集，自动拓扑重构为可交互数字模型。将古籍文字自动解析为分镜脚本，匹配历史素材库，批量生成动态漫画与数字人讲解视频。支持用户上传文物照片或语音描述，定位关联藏品
2	制造业智能体	接入 PLC、SCADA 及设备传感器数据，同步 ERP、MES、WMS 等信息，构建生产数字孪生。构建设备健康度画像，预测故障并自动触发维保工单、调整排程。将订单、产能、工装、物料等约束转化为多目标优化函数，动态生成生产计划。部署工业相机与边缘 AI，在线检测产品瑕疵与尺寸偏差
3	农业智能体	部署田间传感器、气象微站、无人机多光谱与卫星遥感，监测土壤墒情、气象、植被指数与病虫害，构建农田数字底座。融合深度学习与作物生长模型，生成精确到立方米、克级、小时级的个性化农事方案（灌溉、施肥、施药）。结合市场价格数据，运用强化学习预测最优定价与上市窗口，自动匹配企业端或市民端渠道，实现订单农业
4	电商智能体	实时采集搜索趋势、社媒舆情、进出口数据及竞品动态，构建需求预测模型。结合企业产能、利润率和物流成本，自动生成“目标市场—潜力产品—定价策略”三维推荐方案
5	经济监测智能体	对城市宏观经济运行、产业链发展、产业集群与园区布局、重点产业及规上企业发展情况进行监测与分析，提供经济运行态势研判

7.4 城市更新

以城市可持续发展为导向，通过城市智能体整合自然资源监测、能源调度、建筑安全等能力，提升资源利用效率与风险防控水平，推动城市空间结构优化与功能升级，部分应用举例见表4。

表 4 城市智能体在城市更新场景应用举例

序号	应用场景	场景描述
1	资源管理智能体	融合卫星遥感、无人机影像、地面物联网数据，基于 GIS 与 BIM 构建自然资源三维数字孪生，实时监测土地利用、森林蓄积、河流水质等指标。通过深度学习自动识别违规占用耕地、非法采伐、水体污染等异常。整合电力、燃气、热力等数据，构建多能互补能源互联网调度平台，运用混合整数规划与强化学习优化源-网-荷-储协同，实现风光储出力调节、冷热电联供动态控制与需求侧响应

8 城市智能体建设路径

城市智能体应用建设路径包括场景识别、打造高质量数据集、构建AI能力、搭建智能体和智能体运营5个步骤。

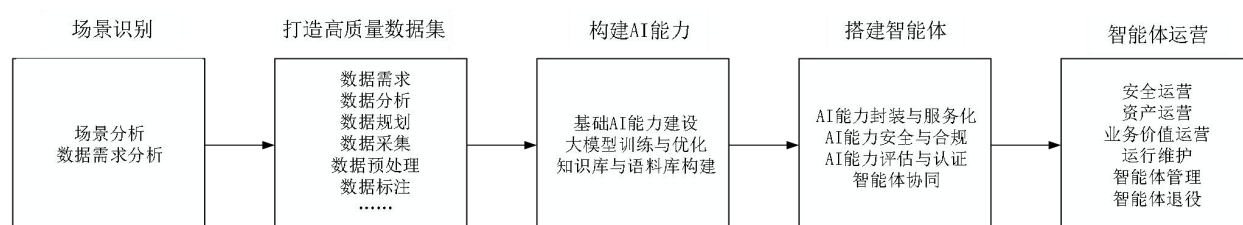


图 1 城市智能体应用建设路径

8.1 场景识别

8.1.1 场景分析

8.1.1.1 场景识别原则

场景识别原则包括：

a) 全面性原则：

- 1) 覆盖城市治理全生命周期，包括规划、建设、管理、运营等各个阶段；
- 2) 涵盖政府、企业、市民等全部利益相关方的需求；
- 3) 统筹考虑城市治理、数字生活、数字经济、城市更新多维度发展目标；

b) 系统性原则：

- 1) 基于城市智能体总体架构，确保场景设计与技术架构的一致性；
- 2) 注重场景间的关联性和协同性，避免孤立建设；
- 3) 遵循从简单到复杂、从局部到整体的渐进式发展路径；

c) 实用性原则：

- 1) 以解决实际问题为导向，聚焦城市治理的痛点难点；
- 2) 充分考虑技术可行性和经济合理性；
- 3) 确保场景应用的可操作性和可持续性；

d) 标准化原则：

- 1) 遵循国家相关技术标准和规范要求；
- 2) 建立统一的场景描述规范和评价体系；
- 3) 确保不同城市间场景的可比较性和可推广性。

8.1.1.2 场景分类体系

场景分类体系包括：

- a) 一级分类（按应用领域）：
 - 1) 城市治理类：
 - 政务服务：网上办事、一网通办、跨域通办等；
 - 应急管理：风险预警、应急指挥、资源调度等；
 - 民意速办：网格管理、服务热线、一表通等；
 - 2) 惠民服务类：
 - 民生服务：教育、医疗、养老、就业等公共服务；
 - 消费服务：智慧商圈、电子商务、消费维权等；
 - 社会保障：社会救助、社会保险、社会福利等；
 - 3) 数字经济类：
 - 产业服务：企业服务、产业链协同、创新孵化等；
 - 智能监测：经济监测、政策服务、企业服务等；
 - 4) 城市更新类：
 - 城市基础设施：城市巡检、车路协同等；
 - 智慧社区：智慧物业、惠民服务、高楼消防等；
- b) 二级分类（按技术复杂度）：
 - 1) 基础级：数据查询、信息展示、简单交互；
 - 2) 应用级：业务办理、流程优化、智能推荐；
 - 3) 智能级：预测分析、决策支持、自动处置；
 - 4) 协同级：跨部门联动、多方协同、一体化服务；
- c) 三级分类（按服务对象）：
 - 1) 市民端：面向个人用户的服务场景；
 - 2) 企业端：面向非政府部门组织的服务场景；
 - 3) 政府端：面向政府部门的行政事务场景。

8.1.1.3 场景优先级评估

场景优先级评估要点包括：

- a) 评估维度：
 - 1) 紧迫性：问题的严重程度和解决的迫切性；
 - 2) 影响面：涉及的用户规模和社会影响范围；
 - 3) 可行性：技术实现难度和资源投入要求；
 - 4) 效益性：预期产生的经济和社会效益；
 - 5) 示范性：对其他场景的引领和带动作用；
- b) 评估方法：
 - 1) 采用层次分析法（AHP）确定各维度权重；
 - 2) 建立评分标准，对每个场景进行量化评估；
 - 3) 综合计算优先级得分，形成场景建设序列。

8.1.2 数据需求分析

8.1.2.1 数据需求分析方法

数据需求分析方法包括：

- a) 场景驱动分析：
 - 1) 输入分析：识别场景运行所需的输入数据；
 - 2) 处理分析：确定数据处理和转换的要求；
 - 3) 输出分析：明确场景产出的数据成果；
 - 4) 反馈分析：分析数据使用效果的反馈机制；
- b) 业务流程分析：
 - 1) 流程梳理：详细描述业务办理的完整流程；
 - 2) 节点分析：识别各流程节点的数据需求；
 - 3) 接口分析：明确系统间的数据交换接口；
 - 4) 异常分析：考虑异常情况下的数据处理需求；
- c) 技术能力分析：
 - 1) 算法需求：分析 AI 算法对训练数据的要求；
 - 2) 模型需求：确定模型训练和推理的数据规模；
 - 3) 性能需求：评估数据处理的性能指标要求；
 - 4) 扩展需求：考虑未来技术发展的数据需求。

8.1.2.2 数据质量要求

数据质量要求包括：

- a) 准确性：
 - 1) 建立数据质量评估指标体系；
 - 2) 设定不同类型数据的准确率阈值；
 - 3) 建立数据校验和纠错机制；
- b) 完整性：
 - 1) 定义数据完整性的评判标准；
 - 2) 建立数据缺失检测和补全机制；
 - 3) 确保关键数据字段的完整性；
- c) 一致性：
 - 1) 统一数据标准和编码规范；
 - 2) 建立数据一致性检查机制；
 - 3) 确保跨系统数据的一致性；
- d) 时效性：
 - 1) 根据业务需求确定数据更新频率；
 - 2) 建立数据时效性监控机制；
 - 3) 确保关键数据的及时更新。

8.1.2.3 数据安全性与隐私保护

数据安全性与隐私保护要求包括：

- a) 数据分类分级：
 - 1) 建立数据分类分级标准；
 - 2) 实施差异化的安全保护措施；
 - 3) 建立数据使用权限管控机制；
- b) 隐私保护技术：

- 1) 采用数据脱敏技术保护个人隐私；
 - 2) 运用差分隐私技术进行数据分析；
 - 3) 实施数据最小化使用原则；
- c) 合规性要求：
- 1) 严格遵守《数据安全法》等法律法规；
 - 2) 建立数据处理合规审查机制；
 - 3) 确保跨境数据传输的合规性。

8.2 打造高质量数据集

高质量数据集建设可参照TC609-5-2025-1，围绕数据需求、数据规划、数据采集、数据预处理、数据标注、模型验证等阶段有序开展。

8.3 构建 AI 能力

8.3.1 概述

城市智能体的AI能力构建是实现智能化城市治理的核心环节，遵循分层构建、能力复用、持续优化的原则，建立涵盖基础算力、模型训练、知识构建的完整AI能力体系。

8.3.2 基础 AI 能力建设

8.3.2.1 算力基础设施

算力基础设施建设要点包括：

- a) 计算资源配置：
 - 1) GPU/TPU 集群：配置 AI 计算能力，按需规划算力规模避免资源冗余；
 - 2) 存储系统：实现高速存储，支持模型和数据的快速读写；
 - 3) 网络架构：建设高带宽、低延迟的内部网络，支持分布式训练；
- b) 云边协同架构：
 - 1) 云端训练中心：承担大模型训练和知识库构建任务；
 - 2) 边缘推理节点：部署在各业务场景，实时 AI 推理服务；
 - 3) 协同调度机制：实现云边资源的统一调度和负载均衡。

8.3.2.2 AI 开发环境

AI开发环境建设要点包括：

- a) 模型开发环境：
 - 1) 支持主流深度学习框架；
 - 2) 提供可视化模型设计和调试工具；
 - 3) 集成自动化机器学习（AutoML 等）能力；
- b) 数据处理工具链：
 - 1) 数据标注平台：支持文本、图像、视频等多模态数据标注；
 - 2) 数据增强工具：提供数据合成、变换、扩充等功能；
 - 3) 特征工程平台：支持特征提取、选择和组合。

8.3.3 大模型训练与优化

8.3.3.1 基础大模型构建

基础大模型构建要点包括：

- a) 预训练模型选择：
 - 1) 通用语言模型；
 - 2) 多模态模型：支持文本、图像、语音的统一理解和生成；
 - 3) 代码生成模型：支持城市治理相关的自动化脚本生成，建立预训练模型选型的适配性、安全性评估标准；
- b) 模型训练策略：
 - 1) 分布式训练：采用数据并行和模型并行相结合的训练方式；
 - 2) 混合精度训练：提升训练效率；
 - 3) 梯度累积和检查点：确保大规模模型训练的稳定性；
 - 4) 训练过程采取数据加密、隔离措施，建立安全审计机制。

8.3.3.2 领域模型微调

领域模型微调要点包括：

- a) 城市治理领域适配：
 - 1) 收集城市管理、公共服务、应急响应等领域的专业语料；
 - 2) 构建领域特定的训练数据集；
- b) 多任务学习框架：
 - 1) 文本理解：支持政策解读、舆情分析、投诉处理等任务；
 - 2) 决策支持：提供资源调度、风险评估、预测分析等能力；
 - 3) 交互对话：实现自然语言的人机交互和多轮对话。

8.3.3.3 模型评估与优化

模型评估与优化要点包括：

- a) 评估指标体系：
 - 1) 准确性指标：精确率、召回率、机器学习 F1 分数等；
 - 2) 效率指标：推理延迟、吞吐量、资源利用率；
 - 3) 安全性指标：对抗攻击防护、隐私保护能力；
- b) 持续优化机制：
 - 1) 在线学习：基于实际应用反馈持续优化模型；
 - 2) A/B 测试：对比不同模型版本的性能表现；
 - 3) 模型蒸馏：将大模型知识迁移到轻量化模型。

8.3.4 知识库与语料库构建

8.3.4.1 城市知识图谱

城市知识图谱要点包括：

- a) 知识体系设计：
 - 1) 实体识别：城市设施、组织机构、人员、事件等；
 - 2) 关系定义：空间关系、时间关系、因果关系、从属关系；
 - 3) 属性描述：静态属性和动态属性的完整刻画；
- b) 知识获取与更新：
 - 1) 结构化数据抽取：从数据库、API 等获取知识；

- 2) 非结构化数据挖掘：从文档、网页、社交媒体提取知识；
- 3) 专家知识录入：录入领域专业知识。

8.3.4.2 多模态语料库

多模态语料库建设要点包括：

- a) 文本语料：
 - 1) 政策法规文档：政策文件和法规条文；
 - 2) 业务流程描述：覆盖城市治理各领域的标准作业程序；
 - 3) 历史案例库：积累典型事件处理案例；
- b) 多媒体语料：
 - 1) 图像数据：城市监控、卫星遥感、无人机航拍等；
 - 2) 音频数据：热线电话、会议录音、现场采集等；
 - 3) 视频数据：监控录像、执法记录、培训材料等。

8.3.4.3 知识质量保障

知识质量保障要点包括：

- a) 质量控制机制：
 - 1) 数据清洗：去除重复、错误、过时的知识条目；
 - 2) 一致性检查：确保知识间的逻辑一致性和完整性；
 - 3) 专家审核：建立专家评审机制，确保知识的准确性；
- b) 版本管理与追溯：
 - 1) 知识版本控制：记录知识的创建、修改、删除历史；
 - 2) 来源追溯：标记知识的来源渠道和可信度等级；
 - 3) 更新机制：建立定期更新和实时更新相结合的机制。

8.4 搭建智能体

8.4.1 AI 能力封装与服务化

8.4.1.1 能力组件化

能力组件化要点包括：

- a) 原子能力：
 - 1) 感知能力：文本理解、图像识别、语音识别等；
 - 2) 认知能力：推理分析、知识问答、决策支持等；
 - 3) 生成能力：文本生成、图像生成、报告生成等；
- b) 能力接口标准化：
 - 1) API 接口规范：定义统一的调用接口和参数格式；
 - 2) 数据格式标准：规范输入输出数据的结构和编码；
 - 3) 服务质量保障：定义响应时间、可用性等 SLA 指标。

8.4.1.2 能力编排与组合

能力编排与组合要点包括：

- a) 智能体架构选型：根据场景复杂度、数据规模、业务协同需求，确定采用多智能体架构或单智能体架构；

- b) 智能体能力开发：开发智能体关键能力，包括意图感知、任务规划、任务执行、持续优化的技术实现；
- c) 功能验证：
 - 1) 通过模拟测试、场景化实测，验证其意图理解、任务规划、调度执行的正确性，目标达成度以及与其他智能体的协同效率；
 - 2) 建立人工干预机制，允许开发与领域专家对智能体的不当决策进行纠正，并以此作为优化其模型的重要反馈数据。

8.4.1.3 能力运营与监控

能力运营与监控要点包括：

- a) 性能监控：
 - 1) 实时监控：监控 AI 服务的调用量、响应时间、错误率；
 - 2) 资源监控：跟踪计算资源、存储资源的使用情况；
 - 3) 业务监控：监控 AI 能力在具体业务场景中的效果；
- b) 运维管理：
 - 1) 自动扩缩容：根据负载自动调整服务实例数量；
 - 2) 故障恢复：提供服务降级、熔断、重试等容错机制；
 - 3) 版本管理：支持 AI 模型和服务的灰度发布和回滚；
- c) 持续学习与优化：基于智能体在运行过程中产生的日志以及接收到的人工反馈，持续优化智能体。

8.4.2 AI 能力安全与合规

8.4.2.1 基础安全

基础安全要求包括：

- a) 网络安全符合 GB/T 22239-2019 中相应等级要求；
- b) 训练数据安全符合 GB/T 45654-2025 中第 4 章的要求；
- c) 数据分类分级符合 GB/T 43697-2024 的要求。

8.4.2.2 感知安全

感知安全要求包括：

- a) 感知数据涉及个人信息保护符合 GB/T 35273-2020 要求，进行脱敏或去标识；
- b) 在各种预期和非预期条件下（如传感器噪声、人为干扰），感知系统都能持续提供完整和准确的信息。

8.4.2.3 协同安全

协同安全要求包括：

- a) 智能体之间通信采用加密协议，如 HTTPS；
- b) 智能体协同需要验证对方智能体身份可信；
- c) 智能体工具调用保证调用接口的安全。

8.4.2.4 执行安全

执行安全要求包括：

- a) 智能体向用户以显著方式明确告知任务执行所申请的操作系统权限、访问用户数据的目的、处理方式等内容，并获得用户许可；
- b) 进行分级安全管控，明确城市治理、公共安全、民生服务等领域的“重要影响任务”范围，智能体执行涉及有重要影响的任务，引入人为因素参加决策并保留决策记录。

8.4.2.5 模型安全

模型安全要求包括：

- a) 对抗攻击防护：
 - 1) 输入验证：对输入数据进行安全检查和过滤，建立异常检测机制；
 - 2) 对抗训练：在训练过程中加入对抗样本提升鲁棒性，按应用场景划分对抗攻击防护等级；
 - 3) 异常检测：识别和拦截恶意输入和异常请求，实时监控模型输入输出；
- b) 隐私保护：
 - 1) 差分隐私：在模型训练中加入噪声保护个人隐私，明确噪声添加合理范围；
 - 2) 联邦学习：支持多方数据协作而不泄露原始数据；
 - 3) 数据脱敏：对敏感数据进行匿名化和脱敏处理。

8.4.2.6 合规管理

合规管理要求包括：

- a) 算法审计：
 - 1) 可解释性：提供模型决策的解释和依据；
 - 2) 透明度：公开模型的基本信息和使用范围；
- b) 数据合规：
 - 1) 数据分类分级：按照敏感程度对数据进行分类管理；
 - 2) 访问控制：实施基于角色的数据访问权限控制；
 - 3) 审计日志：记录数据访问和使用的完整日志；
- c) 评测合规：
 - 1) 搭建智能化评测平台，实现自动化扫描、渗透测试、风险评估等功能；
 - 2) 建立内容安全检测能力，依据监管部门发布的测试数据集开展内容安全合规自查自纠，保障持续满足安全合规要求，可依据 8.4.3.3 的评测要点执行；
- d) 伦理合规：
 - 1) 确保智能体提供的公共服务公平公正，不歧视任何群体；
 - 2) 保障智能体决策过程透明可解释，避免暗箱操作；严格保护个人隐私，避免过度收集和滥用个人信息；
 - 3) 定期评估算法公平性，防止算法歧视和偏见；
 - 4) 算法设计、模型训练和优化、提供服务过程中，采取训练数据筛选、价值观对齐、输出校验、强化学习人类反馈（RLHF）、建立“价值观红线”规则引擎等方式，有效规避产生民族、信仰、国别、地域、性别等歧视的风险；
 - 5) 建立 AI 内容安全围栏，确保输入、输出内容符合社会伦理、国家及地方法律法规的要求。

8.4.3 AI 能力评估与认证

8.4.3.1 能力成熟度评估

能力成熟度评估要点包括：

- a) 评估维度：
 - 1) 技术成熟度：算法先进性、模型性能、系统稳定性；
 - 2) 应用成熟度：场景覆盖度、用户满意度、业务价值；
 - 3) 管理成熟度：治理体系、运营能力、安全保障；
- b) 评估方法：
 - 1) 定量评估：基于客观指标的量化评估；
 - 2) 定性评估：专家评议和用户反馈；
 - 3) 第三方评估：引入独立机构进行客观评估。

8.4.3.2 认证与标准化

认证与标准化要点包括：

- a) 能力认证：
 - 1) 功能认证：验证 AI 能力是否满足功能要求；
 - 2) 性能认证：验证 AI 能力是否达到性能指标；
 - 3) 安全认证：验证 AI 能力是否符合安全标准；
- b) 标准化建设：
 - 1) 技术标准：制定 AI 能力的技术规范和接口标准；
 - 2) 管理标准：建立 AI 能力的管理制度和流程规范；
 - 3) 服务标准：定义 AI 能力的服务质量和交付标准。

8.4.3.3 智能体评测

智能体评测要点包括：

- a) 评测规则：依据相应法律法规及标准规范，制定覆盖城市智能体全生命周期的安全评测规则；
- b) 评测范围：
 - 1) 技术安全评测：包括系统漏洞、数据加密、访问控制、应急响应等；
 - 2) 数据安全评测：包括数据采集、传输、存储、加工、使用、销毁全流程安全；
 - 3) 功能质量评测：包括智能决策准确性、容错能力、抗干扰能力等；
 - 4) 合规性评测：包括法律法规符合性、行业标准符合性等；
- c) 评测机制：
 - 1) 建立定期评测制度，每季度进行常规评测，重大版本更新后进行专项评测；
 - 2) 可引入第三方评测机构，确保评测结果的客观性和公正性；
 - 3) 建立评测结果反馈机制，形成问题整改闭环管理；
 - 4) 根据要求完成 AI 备案并向监管部门开放测试接口，确保所有向公众提供服务的城市智能体符合监管部门相关要求。

8.4.4 智能体协同

实现智能体协同要点包括：

- a) 互操作机制：
 - 1) 语义互操作：形成统一的本体定义和知识表示规范；
 - 2) 数据互操作：支持 JSON-LD 等语义化数据交换格式；
 - 3) 接口互操作：RESTful API/OpenAPI 规范、服务发现机制；
 - 4) 协议互操作：除 MCP/A2A 外，明确协议版本兼容性要求；
- b) 任务管理机制：将复杂目标拆分为原子任务；基于匹配算法将任务分配给智能体；

- c) 设计协作模式：顺序式、监督者和竞争模式；
- d) 冲突解决机制：针对资源冲突、决策冲突和数据冲突时建立解决机制。

8.5 智能体运营

8.5.1 安全运营

8.5.1.1 定期安全评测

定期安全评测要点包括：

- a) 定期开展城市智能体安全测评，可依据 8.4.3.3 的评测规则与机制执行；
- b) 重大版本更新、发生安全事件后开展专项测评；
- c) 对测评不合格的智能体立即暂停运营并限期整改，整改完成后复评合格方可恢复使用；
- d) 对第三方组件、服务和外包环节进行全生命周期管理。包括对供应商进行安全资质评估与定期复评，建立合同中的安全条款与违约责任；同时对上线后的智能体进行动态漏洞扫描与运营安全监控。

8.5.1.2 风险分级分类管理

风险分级分类管理要点包括：

- a) 参考《人工智能安全治理框架 2.0 版》和 GB/T 46347-2025 定义智能体风险的维度与类别，对每个风险类别根据严重程度，定义明确的量化或质化标准及触发条件；
- b) 建立城市智能体安全事件分级应急响应机制，明确处置流程、责任主体与处置时限。

8.5.1.3 运行时防护与异常治理

运行时防护与异常治理要点包括：

- a) 提供“可解释性说明”、“责任回溯日志”，为潜在的行政复议或侵权诉讼保留电子证据，做好智能体侵权责任认定；
- b) 参考相关标准规范建立智能体上线后的非确定性、自主行动、长期运行、行为漂移等特性的监控机制，提供实时拦截和持续监督及适应性调整的能力。

8.5.1.4 伦理安全运营

伦理安全运营要点包括：

- a) 依据《新一代人工智能伦理规范》等文件，制定城市智能体伦理体系，确立公平性、透明性、可解释性、问责性、隐私保护五大伦理原则；
- b) 伦理安全管理机制：
 - 1) 建立伦理安全审查委员会，负责智能体伦理安全评估和决策；
 - 2) 建立伦理安全风险评估制度，在智能体设计、开发、部署各阶段进行伦理评估；
 - 3) 建立伦理安全投诉处理机制，接受公众对智能体伦理问题的投诉和建议。
 - 4) 建立伦理安全审查触发机制，在智能体上线前进行常规审查及定期审查；在模型算法、知识库、数据等出现重大变化或风险信号时立即启动复审；
- c) 伦理安全教育宣传：对智能体开发、运营人员进行伦理安全培训。

8.5.2 资产运营

资产运营要点包括：

- a) 通过安全评测的智能体，注册接入城市智能体资产管理；

- b) 使用智能体资产管理的注册智能体，需要通过订阅或者订购流程。建立基于角色的订阅 / 订购权限管理机制，明确不同用户的使用范围与操作权限。

8.5.3 业务价值运营

业务价值运营要点包括：

- a) 基于城市全域数字化转型的总体目标和指标体系，计算智能体的业务价值，以及对于城市全域数字化转型的贡献度；
- b) 基于业务价值评估结果，对高价值智能体强化资源配置，对低价值、低贡献的智能体进行迭代优化或下线处置，形成智能体资产动态优化机制。

8.5.4 运行维护

运营服务体系构成包括：

- a) 运营管理模块：
 - 1) 智能体运行监控：实时监测智能体系统运行状态、性能指标、资源使用情况；
 - 2) 故障管理：建立故障预警、诊断、修复机制，实现故障快速处置；
 - 3) 性能优化：基于运行数据进行性能分析，优化系统配置和资源分配；
 - 4) 版本管理：负责智能体版本更新、升级、回滚等管理工作，建立智能体版本与全生命周期数据的可追溯机制；
 - 5) 运营反馈与持续改进机制：明确运营数据采集、反馈路径、反馈周期与责任主体。运营数据采集包括性能指标、业务价值指标、用户满意度、安全事件；
- b) 服务保障模块：
 - 1) 服务级别管理：制定服务级别协议（SLA），明确服务可用性、响应时间等指标，保障服务可用性；
 - 2) 客户服务：建立多渠道服务支持体系，提供技术咨询、问题解答等服务；
 - 3) 培训服务：为用户和运维人员提供操作培训、技术培训等。

8.5.5 智能体管理

宜考虑人工智能政策、智能体目标和已识别的风险，分配岗位和职责。需要明确岗位和职责的领域包括：

- 风险管理；
- 智能体影响评估；
- 资产和资源管理；
- 信息安全；
- 物理安全；
- 隐私；
- 开发；
- 绩效；
- 人员监督；
- 供应商关系；
- 合规性；
- 数据质量管理(全生存周期)；

各种岗位的职责宜界定到适合个人履行其职责的程度。

8.5.6 智能体退役

当城市智能体持续产生低价值，且通过升级迭代仍无法满足新的需求，可考虑智能体的下线退役。退役要求包括：

- a) 退役评估：由主管部门联合技术方对智能体的运行效能、技术陈旧度、安全风险等进行综合评估，判断是否达到退役标准。例如，当无法适配新业务需求或存在重大安全隐患时，启动退役流程；
- b) 数据迁移与销毁：对仍在使用价值的数据进行归档迁移，涉及市民隐私、政务机密等敏感信息则按规范彻底销毁，防止数据泄露；
- c) 服务交接：将原由该智能体承担的政务、交通、医疗等服务功能，平稳转移至其他系统或人工机制，确保公共服务不中断；
- d) 系统下线：在确认无业务依赖后，逐步关闭计算资源、断开网络连接，完成物理与逻辑层面的下线操作；
- e) 审计复盘：对整个生命周期进行总结，形成治理经验，用于优化未来智能体的设计与管理。

参 考 文 献

- [1] 关于深化智慧城市发展 推进城市全域数字化转型的指导意见（发改数据〔2024〕660号）
 - [2] 深化智慧城市发展 推进全域数字化转型行动计划（发改数据〔2025〕1306号）
 - [3] 国家数据基础设施建设指引（发改数据〔2024〕1853号）
 - [4] 生成式人工智能服务管理暂行办法
 - [5] 重庆市人工智能赋能超大城市现代化治理三年行动计划（2025—2027年）
 - [6] 中华人民共和国科学技术部 新一代人工智能伦理规范（2021年9月25日）
 - [7] 人工智能安全治理框架2.0版
 - [8] 新一代人工智能伦理规范
 - [9] GB/T 45288.1-2025 人工智能 大模型
 - [10] TC609-4-2026-12 城市全域数字化转型 数字化运营指引
 - [11] TC609-4-2026-10 城市全域数字化转型 城市智能中枢 人工智能公共服务平台总体要求
 - [12] TC609-5-2025-2 高质量数据集 格式要求
 - [13] TC609-5-2025-3 高质量数据集 分类指南
 - [14] TC609-5-2025-4 高质量数据集 质量评测规范
-