ICS 35.240.01
CCS L 72

T/AIIA

团 体 标 准

T/AIIA XXXX—2025

智能体全生命周期构建与管理规范

Standards for the construction and management of the full lifecycle of intelligent agents

（征求意见稿）

2025－XX－XX 发布 2025－XX－XX 实施

深圳市人工智能产业协会 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。

本文件由深圳市迪博技术有限公司提出。

本文件由深圳市人工智能产业协会归口。

本文件起草单位：

本文件主要起草人：

智能体全生命周期构建与管理规范

1 范围

本文件规定了智能体在需求分析、设计规划、开发实施与测试评估、评测及发布等全生命周期阶段的构建与管理规范。

本文件适用于政务领域中智能体的构建、管理、评价与改进活动。

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 22080-2016 信息技术 安全技术 信息安全管理体系 要求

GB/T 36345-2018 信息技术 通用数据导入接口

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能体 agent

能够在特定任务或场景中自主学习、感知、决策并执行操作的人工智能系统。

注1：智能体通过与环境交互实现目标导向的行为，其核心特征包含自主性、环境感知能力、动态决策能力和多智能体协作能力。

注2：智能体体系结构由感知器、信息处理器、决策模块、效应器、知识库、通信模块六个核心模块构成。

[来源：《计算机科学技术名词》，术语编码：08.0146]

3.2

需求分析 requirements analysis

基于用户需求和业务目标，确定智能体的功能、性能、数据需求和实现路径的过程。

注：包括功能需求（如任务处理能力）、非功能需求（如响应时延、安全性）及约束条件（如法规合规性）。

3.3

应用场景 application scenario

智能体应用的具体环境和目标任务，包括但不限于智能体用于支持的业务流程、功能需求及其服务对象。

3.4

平台集成 platform integration

智能体与数字政府人工智能公共支撑平台的对接过程，包括技术接口的适配、数据交互的配置及运行环境的兼容性要求，以确保智能体能够稳定运行并与其他系统高效协作。

4 需求分析

4.1 场景需求分析

具体要求如下：

a） 应明确目标应用场景，包括各类智能业务处理场景，确保智能体的核心功能能够有效解决场景中的特定问题；

b） 应根据目标应用场景识别关键需求，并确保智能体能有效支持解决这些需求；

c） 确保智能体对场景需求的支持，能够在数字政府人工智能公共支撑平台上有效实现，并与平台的整体架构和业务目标一致。

4.2 功能需求分析

具体要求如下：

a） 应根据目标应用场景分析智能体所需的功能模块，例如数据处理、分析决策等，确保这些功能能够满足场景的实际需求并有效解决业务问题；

b） 应根据智能体在实际应用中的需求，定义所需的扩展功能，以保障系统的稳定性和运行效率；

c） 功能需求分析应考虑与数字政府人工智能公共支撑平台其他模块或组件的集成，确保不同功能模块之间的协同工作。

4.3 非功能需求分析

具体要求如下：

a） 应针对智能体的响应时延进行明确界定，根据不同应用场景的实时性要求，制定合理的时延指标；

b） 应高度重视信息安全非功能需求，参照 GB/T 22080-2016《信息技术 安全技术 信息安全管理体系 要求》及相关信息安全标准，构建完善的安全防护体系。需采取数据加密、访问控制、安全审计等措施，保障数据在采集、传输、存储和使用过程中的保密性、完整性和可用性；对智能体的操作行为进行全程记录，确保可追溯，防范未授权访问和数据泄露风险；

c） 应考虑系统的可靠性需求，定义合理的平均无故障运行时间、故障恢复时间等指标，确保智能体在不同负载情况下能够稳定运行，减少因故障导致的业务中断；

d） 应具备可扩展性，在架构设计上预留扩展接口，支持功能模块的增减和处理能力的动态调整，以适应业务规模扩大和技术迭代升级的需求。

4.4 技术需求分析

具体要求如下：

a） 技术架构应符合数字政府人工智能公共支撑平台的环境要求，确保智能体能够稳定运行在平台上；

b） 数据接口应明确智能体所需接入的数据来源、格式及协议标准，接口标准可参考GB/T 36345-2018，确保数据传输的准确性与及时性；

c） 智能体应具备足够的可扩展性，以应对未来需求的增长，并适应可能的技术升级或功能扩展。

5 设计规划

5.1 智能体功能设计

核心设计要点：

a） 应根据目标应用场景设计智能体的核心功能模块，确保每个模块能够有效支持场景需求的实现；

b） 设计时应确保功能模块之间的协调性，避免冗余或冲突，确保智能体能够高效运作；

c） 各功能模块的设计应考虑到可扩展性，以便后续根据需求进行功能增强；

d） 需明确功能模块间的接口定义，包括输入输出数据格式、字符长度约束、字段类型及错误代码定义等，例如接口数据宜采用结构化格式，明确必填字段与可选字段，对超出字符限制或格式不符的情况定义相应错误标识，确保模块间数据交互的准确性和一致性，减少集成过程中的适配问题。

5.2 数据流与处理设计

核心设计要点：

a） 应根据场景需求设计智能体的数据流，包括数据采集、处理、分析与存储环节，确保数据处理的效率与准确性；

b） 设计应确保数据传输的高效性和低延迟，符合数字政府人工智能公共支撑平台的数据接口规范，
确保平台内不同模块间的数据流畅传递；
c） 数据存储方案应根据数据量的增长设计，采用合适的数据库与存储架构，确保数据的高可用性与可扩展性。

5.3 技术架构设计

核心设计要点：
a） 应明确智能体所需的技术架构，包括计算资源、存储、网络等，确保能够支持智能体的正常运行；
b） 架构设计应确保智能体的可靠性和稳定性，避免单点故障，确保在高负载环境下能够稳定运行；
c） 应设计适当的容灾和备份方案，确保在智能体出现故障时能够迅速恢复。

5.4 隐私安全设计

应采用隐私设计原则，确保系统默认配置符合最小权限原则。

6 开发实施与测试评估

6.1 开发模式选择

智能体的开发模式应根据需求和目标应用场景来选择，确保开发工作能够高效且符合实际需求。开发模式分为以下两种：
a） 简易智能体
- 通过页面交互式方式，表达意图，输入应用角色指令，引入知识库、自定义组件等能力创建智能体；
- 此模式适用于零代码基础，需通过页面简单交互进行智能体的功能设计、角色指令和新增知识库等工作。

b） 编排智能体
- 通过拖拽方式快速搭建业务流，结合大模型，知识库，工具等组件，完成智能体开发；
- 此模式适用于低代码基础，通过编制工作画布，定义智能体的工作流程，并对流程基本属性或更多属性进行配置，可修复运行方式、事件、补偿规则等。

6.2 功能模块开发与实现

应根据需求分析和设计规划中的功能定义，进行智能体功能模块的开发与实现。每个模块应具备清晰的功能边界，并符合前期定义的技术和业务标准。开发过程中应重点关注以下五个方面：
a） 功能开发应逐步进行，从核心功能模块开始，确保每个模块在功能实现上无误；
b） 开发过程中，相关人员应对每个功能模块进行详细的实现，确保其功能符合预期；
c） 开发应遵循模块化设计，确保每个功能模块之间的独立性和可维护性；
d） 开发过程需遵循统一的开发规范，包括代码编写规范、版本控制规范、文档撰写规范等，例如代码应添加清晰注释以提升可读性，版本更新需记录变更内容及原因，开发文档需明确模块功能、接口参数及调用方式等，保障开发过程的规范性和可追溯性；
e） 开发过程中应同步考虑商业秘密保护要求，对涉及核心算法、关键数据等商业秘密的代码和文档，需按照涉密载体管理要求进行加密存储、权限管控及流转审批，避免开发阶段的信息泄露。

6.3 安全隐私措施

关键实施要求：
a） 应实现端到端加密传输，对静态数据采用AES-256加密存储，密钥由硬件安全模块管理；
b） 应实施细粒度的访问控制策略，包括基于属性的访问控制(ABAC)和动态权限管理。

6.4 技术实现与平台集成

开发过程中，应确保智能体能够与数字政府人工智能公共支撑平台无缝集成，具体要求包括：

a） 应遵循数字政府人工智能公共支撑平台的技术架构与接口规范，确保智能体能够与平台中的其
他组件协同工作；
b） 应能够高效对接数字政府人工智能公共支撑平台的数据源，满足实时性和准确性要求；
c） 数字政府人工智能公共支撑平台集成过程中，应兼容平台的安全性和性能要求，避免在集成后出现稳定性问题。

7 评测工作

7.1 评测目标与内容

具体包含以下方面：
a） 通过建立评估标准体系，构建多维度的指标评估框架，结合业务专家主观和自动化裁判的客观评估，为用户提供模型、智能体、知识库的综合视图；
b） 评测内容涵盖从基线技术能力到实际应用场景表现的各个方面，确保用户能够清晰了解参评对
象的优缺点，从而做出明智的选择；
c） 智能体评测聚焦于智能体的交互能力、任务执行效率、用户体验和安全性，通过模拟真实场景来衡量其实际表现。

7.2 评测结果与反馈

主要呈现形式如下：
a） 通过评测报告结合专业分析方法，对数据进行深入解读，构建评测报告时会详细列出评测对象的各项评测指标和分析结果，便于用户根据评测结果；
b） 通过评测榜单对评测对象评测后生成的各项关键指标对参评对象进行先后排序，为用户提供了直观、清晰的表现概览，构建榜单时支持参评对象按照业务能力、指标、基线能力等不同维度进行排名，可根据参评综合能力进行排序。此外，评测榜单还能够通过历史数据对比，展示评测对象在不同时间段的表现变化；
c） 通过评测比对分析，用户可以在构建比对任务时将多个评测对象的关键指标并列展示，直观地观察它们在业务能力、指标能力、基线能力等方面的具体差异。

8 智能体发布

智能体发布需确保发布的功能、性能和安全性满足数字政府人工智能公共支撑平台要求，并符合目标应用场景的需求，应遵循以下流程：
a） 发布申请：相关人员需填写发布申请信息，包括但不限于智能体、申请日期、目标应用场景描述，并附上相关附件，确保信息的完整性和可用性；
b） 发布审批：审批人员应对发布申请进行审核，确保智能体符合数字政府人工智能公共支撑平台的合规性要求及业务需求。如果申请不符合要求，审批人员将退回申请并提供修改意见。申请人根据反馈进行修改后重新提交；
c） 自动发布：审批通过后，智能体自动发布至数字政府人工智能公共支撑平台。根据智能体的功能与应用场景，系统会自动进行分类并推送至适当的资源库中，确保目标用户可以访问；
d） 状态更新：实时更新智能体状态，发布成功后状态更新为启用，下架成功后状态变为禁用。

9 政务智能化领域合规要求

9.1 用户协议

具体要求如下：
a） 应清晰界定智能体在政务领域的功能边界，确保在辅助政务决策、信息处理、公众服务等方面的功能描述准确，严禁作出超越其能力范围的承诺；

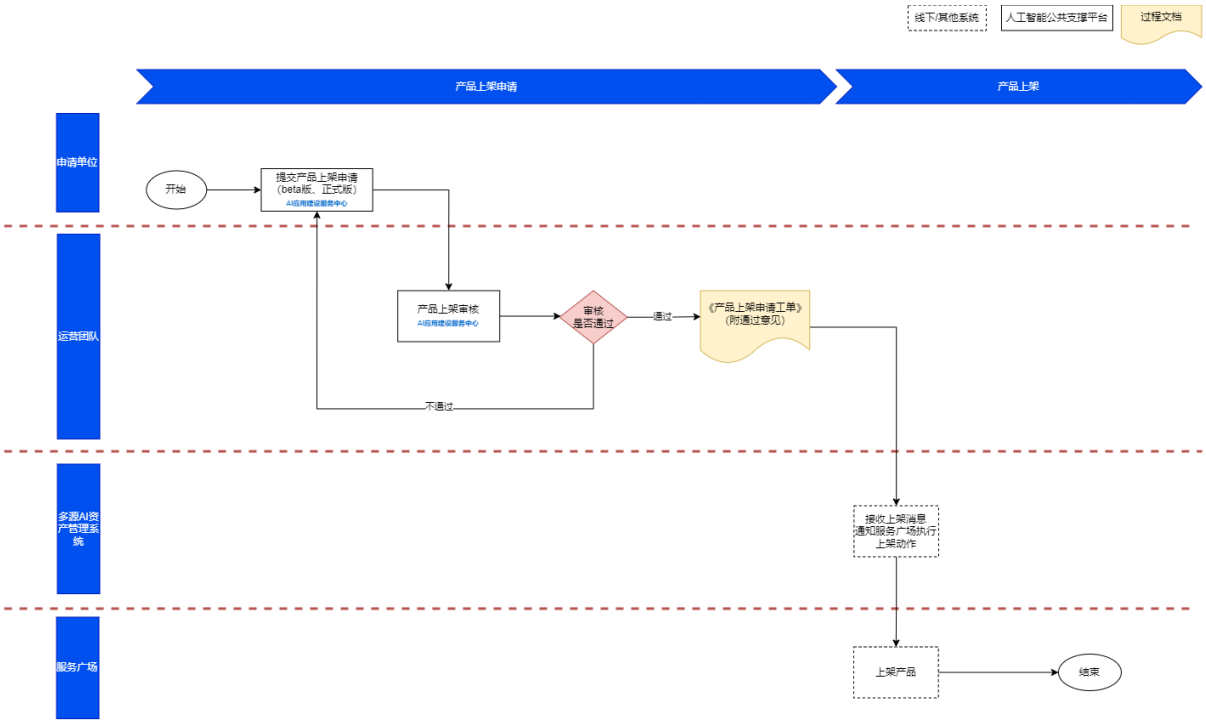
b） 明确是否支持针对政务数据的特定训练或与政务相关的第三方插件集成，若支持，需详细说明相关流程与安全保障措施；
c） 严格明确禁止用途，如严禁利用智能体生成危害国家安全、社会公共安全、违反法律法规以及侵犯公民、法人和其他组织合法权益的内容；严禁将智能体用于自动化恶意攻击政务网络系统、干扰政务正常运行等行为；
d） 制定严格的用户数据提交规范，明确禁止上传未经授权的公民个人隐私数据、国家秘密数据以及敏感政务数据等；
e） 声明用户需对通过智能体生成的内容进行合规性审核，强调用户对生成内容在政务场景中合法、合规使用负责，如“智能体编排工具仅提供辅助生成服务，用户需自行严格审核生成内容是否符合政务工作规范与法律法规要求”；
e） 若提供针对政务内容的审核工具，需明确界定审核失败时各方责任比例，充分考虑政务工作的严肃性与特殊性，保障政务信息的准确性与安全性。

9.2 隐私政策

具体要求如下：

a） 精确明确数据收集范围，针对政务智能化场景，列出收集的输入数据（如公众咨询信息、政务业务数据等）、输出数据（如生成的政务报告、回复内容等）、行为数据（如智能体操作日志、使用频率等），对于涉及公民个人敏感信息（如身份证号、医疗健康信息等）以及重要政务敏感数据需特别声明收集目的、方式与保护措施；
b） 清晰阐述数据用途，如数据用于政务流程优化、提升政务服务质量的训练改进，明确是否会因政务协同等需求共享给其他政务部门或第三方机构，若共享需说明共享原则与安全保障机制。

附 录 A
（规范性）
智能体发布流程图



图A.1 智能体发布流程图

参 考 文 献

［1］ 计算机科学技术名词审定委员会.计算机科学技术名词.2018 年

［2］ 全国人民代表大会.中华人民共和国未成年人保护法.2024 年

［3］ 国家互联网信息办公室、工业和信息化部、公安部、国家广播电视总局.人工智能生成合成内容标识办法.2025 年