

T/ZPMA

团 体 标 准

T/ZPMA 0044—2026

人工智能赋能公共服务智能化应用指南

Guidelines for Artificial Intelligence-Enabled Intelligent Applications in Public
Services

（征求意见稿）

XXXX—XX—XX 发布

XXXX—XX—XX 实施

浙江省职业经理人协会 发 布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 总则 2

5 总体框架 3

6 策划与设计阶段 4

7 实施部署过程通用规范 6

8 技术集成与核心能力要求 8

9 成效评估持续改进框架 10

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XXX提出。

本文件由浙江省职业经理人协会归口。

本文件起草单位：XXX

本文件主要起草人：XXX

人工智能赋能公共服务智能化应用指南

1 范围

本文件规定了人工智能赋能公共服务智能化应用的范围、规范性引用文件、术语和定义、总则、总体框架、策划与设计阶段、实施部署过程通用规范、技术集成与核心能力要求。

成效评估持续改进框架本文件适用于各级各类公共服务提供主体、人工智能技术服务机构、公共服务平台建设与运维单位，开展政务服务、公共法律服务、公共教育、公共医疗、社会保障、社区服务、公共文化、交通出行、应急服务等公共服务智能化应用的规划、设计、建设、运营、管理与效能评价。

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 20984 信息安全技术 信息安全风险评估方法
- GB/T 32169.1 政务服务中心运行规范 第1部分：基本要求
- GB/T 32170.1 政务服务中心标准化工作指南 第1部分：基本要求
- GB/T 34079.2 基于云计算的电子政务公共平台服务规范 第2部分：应用部署和数据迁移
- GB/T 35273 信息安全技术 个人信息安全规范
- GB/T 36344 信息技术 数据质量评价指标
- GB/T 37964 信息安全技术 个人信息去标识化指南
- GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求
- GB/T 40689 智慧城市 设备联接管理与服务平台技术要求
- GB/T 41387 信息安全技术 智能家居通用安全规范
- GB/T 41867 信息技术 人工智能 术语
- GB/T 43697 数据安全技术 数据分类分级规则
- GB/T 45392 数据安全技术 基于个人信息的自动化决策安全要求
- GB/T 45654 网络安全技术 生成式人工智能服务安全基本要求
- GB/T 46483 信息技术 客服型虚拟数字人通用技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

人工智能 artificial intelligence (AI)

人工智能系统相关机制和应用的研究和开发。

[来源：GB/T 41867, 3.1.2]

3.2

公共服务 public service

由政府主导、社会力量参与，为满足公众基本需求而提供的普惠性、公益性、均等化服务活动。

[来源：GB/T 43713, 3.1]

3.3

人工智能赋能公共服务 AI-enabled public service

将人工智能技术与公共服务深度融合，优化服务流程、提升服务效能、扩大服务覆盖、保障服务均等的模式。

3.4

客服型虚拟数字人 customer service virtual digital human

面向特定行业应用，具有开展客户服务功能的虚拟数字人。

[来源：GB/T 46483, 3.2]

3.5

生成式人工智能 generative artificial intelligence

利用生成式人工智能技术向公众提供生成文本、图片、音频、视频等服务。

[来源：GB/T 45654, 3.1]

3.6

多模态交互 multimodal interaction

融合文本、语音、图像、视频、触控等两种及以上交互方式，实现人与系统自然对话的交互模式。

3.7

智慧公共服务平台 smart public service platform

依托人工智能、大数据、云计算等技术，整合公共服务资源，提供一体化、智能化公共服务的信息系统。

4 总则

4.1 总体目标

4.1.1 人工智能赋能公共服务智能化应用应以提升公共服务普惠化、便捷化、智能化水平为核心，依托人工智能技术推动公共服务全流程、全场景优化升级。

4.1.2 人工智能赋能公共服务应用应构建覆盖全面、精准高效、安全合规、均等可及的智能化公共服务体系。

4.1.3 建设主体宜聚焦公共服务资源分布不均、供给效率不高、服务成本偏高等痛点问题，通过技术赋能实现靶向破解。

4.1.4 服务提供方可依托智能化应用扩大服务覆盖范围、保障特殊群体服务权益，支撑 15 分钟公共服务圈落地见效，推动公共服务供给模式从传统人工向智能协同转型，持续提升公众获得感、幸福感与安全感。

4.2 基本原则

4.2.1 以人为本，公益导向

4.2.1.1 服务提供方应坚守公共服务公益性、普惠性、均等化本质属性，以公众实际需求为核心设计应用场景与服务流程。

4.2.1.2 建设主体宜优先适配老年人、青少年、残疾人、偏远地区群众等弱势群体的使用习惯与服务诉求。

4.2.1.3 技术支撑单位可采用多模态、低门槛交互方式，保障全体社会成员平等获取智能化公共服务。

4.2.1.4 所有参与主体应不得违背公益属性，利用智能化公共服务开展商业化牟利活动。

4.2.2 业务牵引，协同增效

4.2.2.1 人工智能赋能公共服务应用应立足公共服务核心业务需求推进技术融合，杜绝技术与业务脱节。

4.2.2.2 政务主管部门宜打破部门、层级、区域间的数据壁垒与服务孤岛，推动多领域公共服务资源协同联动。

4.2.2.3 运营单位可通过智能流程再造、服务联动办理，提升公共服务响应速度与办理效率。

4.2.2.4 基层服务主体应借助智能化应用实现业务提质、基层减负，降低一线服务人员工作负担。

4.2.3 统筹规划，集约建设

4.2.3.1 地方主管部门应遵循统一规划、分级实施、资源共享的思路开展建设，杜绝重复投入与分散建设。

- 4.2.3.2 平台运维单位宜依托现有公共服务平台、政务云、数据中台进行集约化升级改造。
- 4.2.3.3 技术服务商可构建统一的人工智能技术底座与服务接口，推动软硬件、数据、服务能力共享复用。
- 4.2.4 安全可信，稳健可控
 - 4.2.4.1 建设运营主体应严格遵守数据安全、个人信息保护、网络安全等级保护相关规定，落实全流程安全管控要求。
 - 4.2.4.2 算法提供方宜建立人工智能算法合规审查、伦理风险评估与服务纠错机制。
 - 4.2.4.3 安全管理单位可构建安全运维、风险预警、应急处置一体化体系。
 - 4.2.4.4 所有参与主体应保障系统稳定运行、数据安全可控、服务输出合规可靠。
- 4.2.5 开放包容，迭代演进
 - 4.2.5.1 人工智能赋能公共服务应用应坚持技术兼容、接口开放，适配多类型技术与场景融合。
 - 4.2.5.2 运营管理方宜建立需求收集、效果评估、优化升级的闭环迭代机制。
 - 4.2.5.3 建设主体可稳步引入新技术、新模型、新应用，持续适配公共服务需求与技术发展趋势。

5 总体框架

5.1 框架构成

人工智能赋能公共服务智能化应用采用六层一体、纵向贯通、横向协同的总体架构，以公共服务业务需求为核心导向，自下而上分为基础设施层、数据资源层、人工智能能力层、智能化应用层、服务与业务场景层，治理、安全与标准体系全面贯穿各层级，形成底座支撑、能力赋能、应用落地、场景服务、全程管控的一体化架构，见图1。

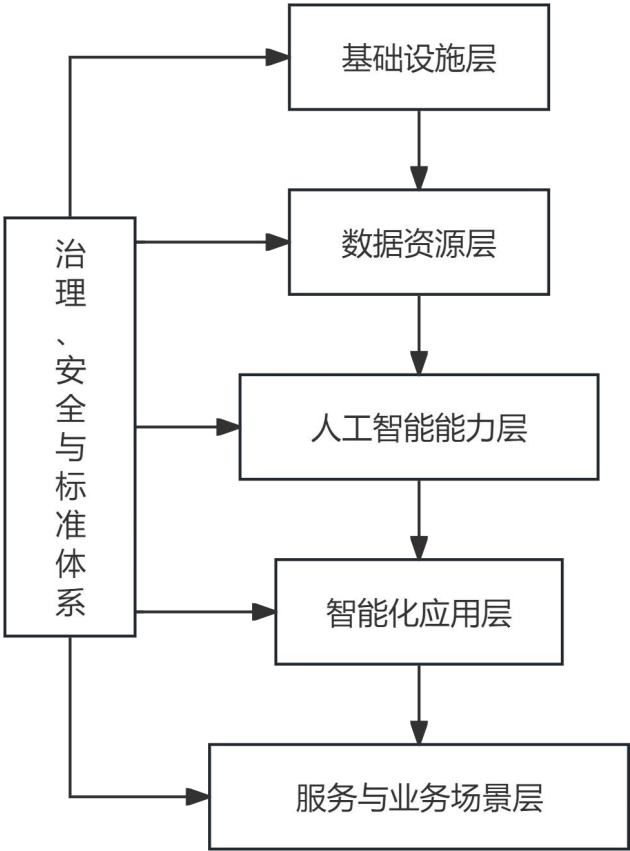


图 1 总体架构图

5.2 层级说明

5.2.1 服务与业务场景层

5.2.1.1 业务主管部门应统筹政务服务、公共法律服务、公共教育、公共医疗、社会保障、社区服务、公共文化、交通出行、应急服务等全领域业务场景，实现公共服务全覆盖。

5.2.1.2 服务提供方宜聚焦老年人、青少年、残疾人、偏远地区群众等重点群体，定制适配化服务场景与服务流程。

5.2.1.3 基层实施单位可依托智能终端、移动设备延伸服务触点，支撑 15 分钟公共服务圈落地。

5.2.1.4 场景运营主体应保障服务场景的公益性、均等性与可及性，不得设置不合理使用门槛。

5.2.2 智能化应用层

5.2.2.1 应用建设主体应开发智能咨询、智能导办、智能宣教、智能匹配、人工转接、自助办理等核心应用功能，满足公共服务办理需求。

5.2.2.2 终端适配单位宜实现 PC 端、移动端、数字大屏、自助终端、物联网设备的多端协同与一体化服务。

5.2.3 人工智能能力层

5.2.3.1 技术提供方应提供公共服务垂直大模型、多模态交互、智能语义理解、知识图谱检索等基础智能能力。

5.2.3.2 数智人研发单位宜提供公共服务数智人形象定制、交互优化、服务适配等专项能力。

5.2.3.3 内容生成主体可运用生成式 AI 技术，快速生产文本、视频、漫画、语音等轻量化服务内容。

5.2.3.4 算法运营单位应持续优化智能推荐、需求识别、案件匹配等算法，提升服务精准度。

5.2.3.5 能力开放平台宜提供标准化接口，支持上层应用快速调用、模块化集成与灵活扩展。

5.2.4 数据资源层

5.2.4.1 数据管理单位应按照 GB/T 43697 要求开展公共数据分类分级，汇聚政策库、案例库、业务库、用户行为数据等核心资源。

5.2.4.2 数据共享主体宜建立跨部门、跨区域数据合规交换机制，保障数据按需、安全、有序共享。

5.2.4.3 数据治理单位应开展数据清洗、脱敏、标注、质量校核，提升数据可用性与安全性。

5.2.4.4 数据使用方应遵循最小必要原则，仅为提供公共服务目的使用数据，严禁超范围采集与滥用。

5.2.5 基础设施层

5.2.5.1 基础设施运维单位应提供云计算、网络、存储、算力、物联网终端等基础资源，保障系统稳定运行。

5.2.5.2 云服务提供方宜依托政务云、行业云开展集约化部署，降低建设与运维成本。

5.2.5.3 基层支撑单位可配置边缘计算设备，提升偏远地区、基层站点的服务响应速度。

5.2.6 治理、安全与标准体系

5.2.6.1 治理监管机构应建立全流程运营治理、算法伦理审查、服务效能评估机制，实现全层级管控。

5.2.6.2 安全责任单位应落实数据安全、个人信息保护、网络安全等级保护等法定要求，构建全方位安全防护体系。

5.2.6.3 标准实施主体宜依据本文件及相关国家、行业标准，统一建设、运行、服务与评价要求。

5.2.6.4 应急管理单位可建立风险预警、应急处置、故障恢复、安全审计的闭环管控机制。

6 策划与设计阶段

6.1 概述

6.1.1 策划与设计是人工智能赋能公共服务智能化应用的前置核心阶段，建设主体应系统开展需求研判、方案设计、规划论证，形成全周期建设实施依据。

6.1.2 策划与设计阶段宜遵循需求导向、科学论证、集约高效、合规可控的思路，统筹业务、技术、数据、资源、风险等核心要素，避免盲目建设与资源浪费。

6.1.3 策划与设计成果可作为项目立项、招投标、建设实施、验收评价的核心依据。

6.2 需求识别与可行性分析

6.2.1 业务需求识别

6.2.1.1 业务主管部门应梳理公共服务法定职责、核心业务流程、高频办理事项，明确智能化改造的业务痛点与堵点。

6.2.1.2 需求调研单位宜对照 GB/T 32169.1、GB/T 32170.1 要求，开展跨部门业务协同需求摸排，厘清服务边界与协同规则。

6.2.1.3 基层服务单位可收集一线服务人员实操需求，确保业务需求贴合实际办理场景。

6.2.2 用户需求调研

6.2.2.1 服务提供方应面向社会公众、企业主体、特殊群体开展分层分类需求调研，覆盖使用习惯、服务偏好、交互诉求。

6.2.2.2 调研实施单位宜采用问卷、访谈、实地踏勘等多种方式，保障需求样本的全面性与代表性。

6.2.3 可行性分析

6.2.3.1 项目论证单位应从政策合规性、技术成熟度、数据可得性、运维可持续性四维度开展综合可行性论证。

6.2.3.2 可行性分析应包含现有系统兼容、资源匹配、安全可控等核心内容，形成专项论证报告。

6.3 目标与价值定位

6.3.1 建设目标设定

6.3.1.1 建设主体应设定可量化、可考核、可落地的建设目标，涵盖服务效率、覆盖范围、成本管控、群众满意度等维度。

6.3.1.2 目标设定宜符合区域公共服务发展规划，与 15 分钟公共服务圈、智慧政务建设等重点工作衔接。

6.3.1.3 远期目标可明确技术迭代、场景拓展、能力升级的方向，保障建设持续性。

6.3.2 价值维度定位

6.3.2.1 项目实施单位应明确公益价值、效率价值、均等价值三大核心定位，坚守公共服务普惠属性。

6.3.2.2 价值定位宜突出对弱势群体、基层一线、偏远地区的服务赋能，体现公共服务均等化要求。

6.4 解决方案业务设计

6.4.1 整体解决方案设计

6.4.1.1 设计单位应基于需求与目标，编制一体化解决方案，明确建设内容、实施路径、交付成果。

6.4.1.2 解决方案宜统筹业务、技术、数据、安全、运维五大模块，形成全链条设计方案。

6.4.1.3 跨区域项目可采用“统一框架、分级适配”的方案模式，兼顾标准化与本地化。

6.4.2 业务流程优化设计

6.4.2.1 业务设计主体应开展现有业务流程再造，简化办理环节、压缩办理时限、减少材料提交。

6.4.2.2 流程优化宜遵循一网通办、一窗受理、并联办理的原则，提升公共服务办理效率。

6.4.2.3 业务设计主体宜依托人工智能与数据共享能力，推进材料免提交、数据自动核验、流程智能流转，降低人工操作成本。

6.4.2.4 流程优化成果应形成标准化业务流程图与办理规范，明确各环节权责、办理时限与数据交互规则，保障流程可执行、可追溯、可监管。

6.4.3 服务场景适配设计

6.4.3.1 场景设计单位应结合不同公共服务领域，定制化设计智能化服务场景，避免通用化套用。

6.4.3.2 针对老年人、残疾人等群体，宜设计适老化、无障碍化服务场景与交互模式。

6.5 技术架构与数据规划

6.5.1 技术架构选型

- 6.5.1.1 技术设计单位应依据 GB/T 41867 要求，选择成熟、稳定、兼容的人工智能技术与架构方案。
- 6.5.1.2 架构选型宜依托现有政务云、行业云平台，采用微服务、模块化架构，保障扩展性与兼容性。
- 6.5.1.3 基层轻量化项目可选用边缘计算、轻量化模型，降低技术部署门槛。

6.5.2 数据资源规划

- 6.5.2.1 数据规划单位应开展数据资源盘点、分类、确权，明确数据来源与使用规则。
- 6.5.2.2 数据规划应包含数据采集、汇聚、治理、共享、脱敏全流程设计，保障数据合规可用。
- 6.5.2.3 涉及个人信息的数据，宜遵循 GB/T 35273 最小必要原则，规划隐私保护技术措施。

6.5.3 接口集成设计

- 6.5.3.1 集成设计单位应依据 GB/T 40689 要求，设计标准化数据接口与服务接口，实现跨系统互联互通。
- 6.5.3.2 接口设计宜兼顾安全性与开放性，支持后续第三方系统接入与功能扩展。

6.6 项目综合规划

6.6.1 资源配置规划

- 6.6.1.1 项目管理单位应统筹人力、设备、技术、服务四类资源，明确各参与方职责分工。
- 6.6.1.2 资源配置宜优先盘活现有存量资源，减少新增硬件与软件的重复投入。

6.6.2 预算与成本管控

- 6.6.2.1 预算编制单位应科学测算建设、运维、升级全周期成本，形成明细预算方案。
- 6.6.2.2 成本管控宜建立集约化投入机制，优先选择性价比高、可持续性强的技术方案。

6.6.3 风险识别与防控

- 6.6.3.1 风险管控单位应识别技术风险、数据风险、合规风险、运维风险，建立风险清单。
- 6.6.3.2 针对核心风险，应制定分级防控措施与应急处置预案，保障项目平稳推进。
- 6.6.3.3 项目实施过程中宜定期开展风险复盘，动态调整防控策略。

6.6.4 实施计划进度管控

- 6.6.4.1 项目实施单位应编制全周期实施计划，明确需求确认、设计开发、集成测试、上线试运行、正式运营等关键阶段与里程碑节点。
- 6.6.4.2 进度管理主体宜建立阶段管控与动态跟踪机制，对关键路径任务进行重点保障。
- 6.6.4.3 跨部门、跨区域协同项目可建立定期会商机制，及时协调解决进度梗阻问题。
- 6.6.4.4 项目验收前应预留充分的试运行与优化周期，确保系统稳定后再正式投入使用。

7 实施部署过程通用规范

7.1 项目组织与协同

7.1.1 组织架构搭建

- 7.1.1.1 项目建设单位应组建跨部门、跨主体的专项实施团队，明确项目总负责人、业务负责人、技术负责人、安全负责人。
- 7.1.1.2 实施团队宜覆盖业务主管部门、技术开发单位、数据提供单位、平台运维单位、基层服务单位。
- 7.1.1.3 关键岗位人员应具备相应的业务能力、技术能力与安全管理能力。

7.1.2 协同工作机制

- 7.1.2.1 牵头实施单位应建立周调度、月通报、重大事项即时会商的协同机制。
- 7.1.2.2 跨部门协同项目宜搭建统一协同工作台，实现需求、进度、问题、成果线上闭环管理。

7.2 开发与集成流程

7.2.1 开发过程管控

- 7.2.1.1 技术开发单位应遵循模块化、低耦合、高可用原则开展代码开发与功能实现。
- 7.2.1.2 开发过程宜执行代码评审、安全扫描、功能自检等过程管控要求。
- 7.2.1.3 开发成果应满足多终端适配、多场景兼容、无障碍交互等公共服务要求。
- 7.2.1.4 开发文档应同步完善，确保系统可维护、可迭代、可交接。

7.2.2 系统集成适配

- 7.2.2.1 集成单位应开展系统对接、接口联调、数据互通、业务贯通等集成工作。
- 7.2.2.2 系统集成宜满足下列要求：
 - a) 兼容政务云、行业云、边缘节点等多种基础设施环境；
 - b) 支持与上级公共服务平台、公共数据共享平台无缝对接；
 - c) 保障跨部门业务流程连贯、数据一致、服务无断点。

7.2.3 版本迭代管理

- 7.2.3.1 开发单位应建立版本号管控、更新日志留存、回滚预案完备的版本管理机制。
- 7.2.3.2 版本更新宜采用小步快跑、灰度发布模式，降低对在线服务的影响。

7.3 数据治理与准备

7.3.1 数据采集

- 7.3.1.1 数据提供单位应依据项目需求合规采集业务数据、政策法规库、案例库、知识库等数据资源。
- 7.3.1.2 数据汇聚应遵循“一数之源、按需归集”原则，避免重复采集、多头采集。
- 7.3.1.3 采集过程应留存来源说明与授权依据，确保数据合法可溯。

7.3.2 数据预处理与质量管控

- 7.3.2.1 数据处理单位应开展数据清洗、格式转换、去重、补全、标准化等预处理工作。
- 7.3.2.2 数据管理单位应依据 GB/T 36344 开展数据完整性、准确性、时效性、一致性校验。
- 7.3.2.3 不合格数据应退回整改，严禁带入模型训练与线上服务环节。
- 7.3.2.4 预处理全过程应留痕，形成可审计的数据处理日志。

7.3.3 数据脱敏处理

- 7.3.3.1 涉及个人信息与敏感公共数据的处理，应严格执行 GB/T 35273 要求，采取脱敏、加密、去标识化措施。
- 7.3.3.2 数据处理操作应做到权限最小化、操作可监控、风险可阻断。

7.4 模型开发与管理

7.4.1 模型训练与优化

- 7.4.1.1 模型研发单位应使用合规、高质量、无偏见数据集开展公共服务垂直领域模型训练。
- 7.4.1.2 模型训练宜针对老年人、青少年、残疾人等群体开展交互适配与话术优化。
- 7.4.1.3 模型应满足响应时延、识别准确率、服务稳定性等预设指标。

7.4.2 模型评估与验证

- 7.4.2.1 模型评估单位应开展功能效果、安全合规、伦理偏见、并发性能多维度验证。
- 7.4.2.2 评估内容宜覆盖：
 - a) 语义理解与智能问答准确率；
 - b) 内容输出合法性、客观性、无歧视性；

- c) 高并发、大流量场景下的服务可用性;
- d) 异常输入与恶意诱导的防御能力。

7.4.3 模型上线与运行维护

- 7.4.3.1 模型上线前应通过安全审查、业务验收、伦理评估,未通过者不得投入服务。
- 7.4.3.2 运维单位应建立模型监控、漂移检测、异常响应、快速迭代的闭环机制。
- 7.4.3.3 模型输出应可解释、可追溯、可审计,关键服务场景宜保留人工复核环节。

7.5 系统测试部署

7.5.1 全维度测试

- 7.5.1.1 测试单位应开展功能测试、性能测试、安全测试、兼容性测试、业务场景全流程测试。
- 7.5.1.2 测试用例应覆盖高频事项、特殊群体、异常流程、边界场景、高并发场景。
- 7.5.1.3 测试发现的缺陷应分级管理,高风险缺陷整改完毕后方可进入下一阶段。
- 7.5.1.4 测试完成后应出具完整测试报告,作为上线依据。

7.5.2 分阶段部署

- 7.5.2.1 部署单位应采用试点先行、分批上线、逐步扩面的渐进式部署策略。
- 7.5.2.2 部署过程应保障服务不中断、数据不丢失、权限不混乱、配置不冲突。
- 7.5.2.3 部署完成后应开展现场验证与链路检查,确保服务可用。

7.5.3 试运行与优化

- 7.5.3.1 系统正式上线前宜开展不少于1个月的试运行,面向真实用户开放服务。
- 7.5.3.2 试运行期间应持续收集用户反馈、运行指标、异常日志。
- 7.5.3.3 试运行问题应逐项整改,形成试运行报告并通过验收后方可转入正式运行。

7.6 变更管理与质量控制

7.6.1 变更全流程管控

- 7.6.1.1 项目实施中需求、技术、数据、架构、流程的变更,应履行申请—评估—审批—执行—核验闭环流程。
- 7.6.1.2 重大变更应组织业务、技术、安全三方评审,必要时邀请外部专家参与。
- 7.6.1.3 变更执行后应开展回归测试,确认不影响现有功能与服务稳定性。
- 7.6.1.4 所有变更应留存记录,纳入项目档案统一管理。

7.6.2 质量监督与核查

- 7.6.2.1 质量管控单位应定期对开发、集成、测试、部署、数据处理各环节开展质量抽查。
- 7.6.2.2 抽查内容应包括代码规范、接口合规、数据安全、功能达标、交互体验、服务效能。

7.6.3 问题闭环整改

- 7.6.3.1 发现的质量缺陷、运行故障、安全隐患应建立台账,明确责任人、整改措施、完成时限。
- 7.6.3.2 整改完成后应复核验证,实现“发现—整改—复核—销号”全闭环。
- 7.6.3.3 典型问题应纳入复盘总结,避免同类问题重复发生。

8 技术集成与核心能力要求

8.1 共性人工智能技术能力指引

8.1.1 多模态交互能力

- 8.1.1.1 技术支撑单位应具备文本、语音、图像、视频融合交互能力,支撑公众自然化服务咨询与办理。

- 8.1.1.2 交互系统宜适配方言、口语化、慢语速表达，适配老年人、基层群众使用习惯。
- 8.1.1.3 多模态模块可支持离线语音识别、弱网环境交互，保障偏远地区服务连续性。
- 8.1.1.4 交互过程应留存必要日志，满足合规审计与问题追溯要求。

8.1.2 智能理解与生成能力

- 8.1.2.1 智能服务系统应具备公共服务领域语义理解、意图识别、逻辑判断能力。
- 8.1.2.2 生成式 AI 模块宜输出合规、准确、通俗的服务内容，杜绝错误引导与违规信息。
- 8.1.2.3 内容生成能力可支持政策解读、流程指引、风险提示等多类型公共服务素材生产。

8.1.3 智能匹配能力

- 8.1.3.1 系统应基于用户需求与业务规则，实现服务事项、资源、办理渠道的智能匹配。
- 8.1.3.2 智能推荐模块宜遵循最小干预原则，仅推送与用户需求相关的公共服务信息。

8.1.4 知识图谱应用能力

- 8.1.4.1 知识图谱构建单位应整合政策、流程、案例、机构、人员等公共服务核心知识。
- 8.1.4.2 知识图谱应建立实体关联、规则推理、路径查询能力，支撑智能问答与深度解读。
- 8.1.4.3 知识图谱宜定期更新迭代，同步最新政策、业务流程与服务资源变化。
- 8.1.4.4 知识图谱可对接智能应用层，为检索、匹配、解读提供统一知识支撑。
- 8.1.4.5 知识管理主体应建立图谱质量核查机制，保障知识准确、权威、无歧义。

8.2 人工智能平台要求

8.2.1 平台架构要求

- 8.2.1.1 人工智能平台应采用微服务、容器化架构，支持高可用、易维护、快速扩展。
- 8.2.1.2 平台宜兼容政务云、行业云部署环境，符合 GB/T 34079.2 相关技术规范。
- 8.2.1.3 平台可提供统一管控界面，实现能力监控、日志审计、异常告警一体化管理。

8.2.2 模型管理要求

- 8.2.2.1 平台应提供模型接入、训练、评估、发布、版本管控全生命周期管理能力。
- 8.2.2.2 模型运行宜具备漂移监测、效果评估、自动优化能力，保障服务持续稳定。
- 8.2.2.3 敏感场景模型应经过安全与伦理审查，未通过评估不得上线运行。
- 8.2.2.4 模型运行日志应完整留存，满足可解释、可追溯、可审计的监管要求。

8.2.3 工具适配要求

- 8.2.3.1 平台宜集成数据标注、模型测试、内容审核、交互优化等配套工具。
- 8.2.3.2 工具组件应降低技术门槛，支持业务人员快速配置服务场景。

8.2.4 接口开放要求

- 8.2.4.1 平台应提供标准化 API 接口，支持与业务系统、终端设备、数据平台对接。
- 8.2.4.2 接口宜具备权限控制、流量管控、日志记录能力，保障对接安全可控。
- 8.2.4.3 接口文档应完整规范，便于第三方机构快速集成与二次开发。
- 8.2.4.4 接口性能应满足高并发调用需求，避免成为服务瓶颈。
- 8.2.4.5 接口升级应兼容历史版本，保障已对接系统平稳运行。

8.3 数据平台与管理要求

8.3.1 数据汇聚整合

- 8.3.1.1 数据平台应归集公共服务业务数据、政策数据、知识库、用户行为数据等核心资源。
- 8.3.1.2 数据汇聚宜遵循一数之源、按需归集，避免重复采集与数据冗余。
- 8.3.1.3 跨部门数据可通过共享交换平台实现合规接入，保障数据来源可溯。
- 8.3.1.4 数据汇聚过程应进行权限校验，严禁非法获取非授权数据。

8.3.2 数据治理管控

- 8.3.2.1 数据管理单位应依据 GB/T 36344 开展数据质量校验，保障数据完整、准确、及时、一致。
- 8.3.2.2 数据治理应覆盖清洗、脱敏、标准化、质量稽核全流程。
- 8.3.2.3 治理过程宜全程留痕，形成可审计、可追溯的数据管理日志。

8.3.3 数据共享交换

- 8.3.3.1 数据平台应按照 GB/T 39477 实行分类分级，支撑跨部门安全共享。
- 8.3.3.2 共享交换宜采用授权、核验、审计三重管控，防止数据越权使用。

8.3.4 数据安全存储

- 8.3.4.1 平台应采用加密存储、权限隔离、备份恢复机制，保障数据存储安全。
- 8.3.4.2 敏感个人信息应遵循 GB/T 37964 要求，采取去标识化、加密存储措施。
- 8.3.4.3 数据存储可支持冷热分离，兼顾性能与成本优化。
- 8.3.4.4 存储环境应符合网络安全等级保护要求，定期开展安全检测。
- 8.3.4.5 数据备份应执行多副本、异地存储策略，防止数据丢失与损坏。

8.4 系统非功能性要求

8.4.1 安全合规要求

- 8.4.1.1 系统应符合网络安全等级保护 2.0 要求，落实身份认证、访问控制、安全审计措施。
- 8.4.1.2 系统宜建立恶意攻击、数据泄露、服务滥用的主动防御机制。
- 8.4.1.3 涉及个人信息处理，应严格遵守个人信息保护相关法律法规与标准规范。
- 8.4.1.4 系统应定期开展安全渗透测试与漏洞扫描，及时修复安全隐患。

8.4.2 性能指标要求

- 8.4.2.1 核心服务响应延时应控制在合理范围，智能问答、查询操作宜秒级响应。
- 8.4.2.2 系统应支持高并发访问，满足区域内公众集中使用需求。
- 8.4.2.3 终端加载、页面渲染宜优化适配，降低弱网环境使用门槛。

8.4.3 可靠性要求

- 8.4.3.1 系统年度服务可用性应达到公共服务类系统要求，保障常态化稳定运行。
- 8.4.3.2 平台宜具备故障自动切换、数据自动备份、快速恢复能力。
- 8.4.3.3 关键组件可采用冗余部署，避免单点故障导致服务中断。
- 8.4.3.4 系统应具备断电保护、网络中断自愈能力，降低意外故障影响。
- 8.4.3.5 运维单位应建立 7×24 小时监控机制，及时发现并处置异常问题。

8.4.4 可扩展性要求

- 8.4.4.1 系统架构应支持业务场景、用户规模、功能模块的灵活扩展。
- 8.4.4.2 平台宜预留第三方 AI 能力、新终端设备、新业务流程的接入空间。

8.4.5 易用性与无障碍要求

- 8.4.5.1 系统界面应简洁清晰、操作便捷，符合公众使用习惯。
- 8.4.5.2 宜提供适老化、无障碍交互模式，支持大字体、语音播报、屏幕阅读器适配。
- 8.4.5.3 基层与老年用户可享受简化流程、引导式操作，降低使用难度。
- 8.4.5.4 交互流程应减少冗余步骤，避免复杂表单与专业术语，提升群众体验。

9 成效评估持续改进框架

9.1 成效评估体系

9.1.1 评估维度指标

9.1.1.1 评估实施单位应构建“服务效能、用户体验、技术性能、合规安全、成本效益”五大核心评估维度，全面覆盖项目建设与运行成效。

9.1.1.2 各维度应设定可量化、可落地的评估指标，核心指标包括但不限于：

- 服务效能：事项办理时限压缩率、服务覆盖率、跨部门协同办结率；
- 用户体验：公众满意度、特殊群体适配率、服务投诉率；
- 技术性能：系统响应时延、服务可用性、模型准确率；
- 合规安全：数据合规率、安全漏洞整改率、隐私保护达标率；
- 成本效益：建设运维成本降低率、人力投入减少量。

9.1.1.3 指标设定宜结合区域公共服务发展水平，兼顾统一性与本地化适配，避免“一刀切”。

9.1.1.4 评估指标应动态更新，同步适配政策调整、技术发展与用户需求变化。

9.1.2 评估方法与流程

9.1.2.1 评估单位应采用定量与定性相结合的评估方法，确保评估结果客观准确。

9.1.2.2 核心评估方法应包括：

- 定量评估：数据统计分析、性能测试、成本核算、用户问卷统计；
- 定性评估：专家评审、用户访谈、业务部门验收、第三方独立评估。

9.1.2.3 评估流程应遵循“准备—实施—分析—报告—整改”闭环，明确各阶段时间节点与责任主体。

9.1.2.4 评估周期宜设定为每半年一次常规评估、每年一次全面评估，重大变更后可开展专项评估。

9.1.2.5 评估成果应形成正式评估报告，明确成效亮点、存在问题及改进建议，作为持续优化的核心依据。

9.2 安全伦理可信保障

9.2.1 安全隐私保护

9.2.1.1 保障主体应建立常态化安全评估机制，定期开展网络安全、数据安全、模型安全专项检测，符合 GB/T 20984 相关要求。

9.2.1.2 应持续强化敏感个人信息保护，严格落实去标识化、加密存储、权限管控措施，杜绝数据泄露、滥用风险。

9.2.1.3 宜建立安全应急演练机制，每季度开展一次应急处置演练，提升安全事件响应与处置能力。

9.2.2 算法公平性与透明度

9.2.2.1 算法管理单位应定期开展算法公平性评估，排查性别、年龄、地域、身份等方面的歧视性偏差。

9.2.2.2 公共服务核心算法宜公开算法原理、决策逻辑与适用范围，保障用户的知情权与监督权，符合 GB/T 45392 要求。

9.2.2.3 算法优化应优先解决公平性问题，对存在偏差的算法及时迭代调整，确保服务均等无歧视。

9.2.2.4 应建立算法投诉反馈机制，及时响应用户对算法决策的异议，开展复核与优化。

9.2.3 人类监督与问责

9.2.3.1 关键服务场景，包括如审批、执法辅助、风险判定等应保留人类监督环节，严禁完全依赖 AI 做出最终决策。

9.2.3.2 应明确 AI 服务相关责任主体，建立“谁开发、谁负责，谁运营、谁负责”的问责机制。

9.2.3.3 对 AI 服务引发的错误决策、安全事故，应开展责任追溯，依法依规追究相关单位与人员责任。

9.2.3.4 宜建立人类监督人员培训机制，提升其对 AI 输出结果的审核、判断与纠错能力。

9.3 运营监测与持续优化

9.3.1 运营监控

9.3.1.1 运营单位应建立 7×24 小时全维度监控体系，覆盖系统运行、模型性能、服务质量、数据安全等核心环节。

9.3.1.2 监控内容应包括：

- 系统层面：服务器负载、网络带宽、服务可用性、故障告警；
- 模型层面：响应速度、识别准确率、漂移情况、异常输出；
- 服务层面：办理量、用户反馈、投诉情况、服务瓶颈。

- 9.3.1.3 应建立分级告警机制，对重大异常情况即时推送、快速处置，避免服务中断。
- 9.3.1.4 监控日志应完整留存，留存期限不少于1年，满足合规审计与问题追溯需求。

9.3.2 模型迭代系统优化

- 9.3.2.1 模型运维单位应建立常态化迭代机制，结合用户反馈、数据更新、评估结果，每季度开展一次模型优化。
 - 9.3.2.2 系统优化应聚焦服务痛点，优先解决响应慢、适配差、操作复杂等用户反映强烈的问题。
 - 9.3.2.3 优化过程应遵循“小步迭代、灰度发布”原则，避免影响现有服务正常运行。
 - 9.3.2.4 优化完成后应开展效果验证，确保优化措施有效，且不引入新的安全隐患与功能缺陷。
 - 9.3.2.5 应建立优化档案，记录优化内容、实施过程、效果评估，形成“评估—优化—验证”的闭环管理。
-