

团 体 标 准

T/SZS XXXX—XXXX

政务辅助智能机器人技术架构要求

Requirements for the technical architecture of government
affairs-assisted intelligent robots

（征求意见稿）

2026-XX-XX 发布

2026-XX-XX 实施

深圳市深圳标准促进会 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 缩略语 1

5 基本要求 1

6 技术架构 2

7 技术能力要求 3

8 前端交互要求 4

9 数据资源要求 4

10 安全保障要求 6

11 风险控制 6

参考文献 错误！未定义书签。

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。

本文件由深圳市福田区政务服务和数据管理局提出。

本文件由深圳市深圳标准促进会归口。

本文件起草单位：XXXX。

本文件主要起草人：XXXX。

政务辅助智能机器人技术架构要求

1 范围

本文件规定了政务辅助智能机器人的基本要求、技术架构、技术能力要求、前端交互要求、数据资源要求、安全保障要求、风险控制等内容。

本文件适用于政务辅助领域的智能机器人技术研发和服务。

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 43697 数据安全技术 数据分类分级规则
GB/T 45301 服务机器人云平台分类及参考体系结构
GB/T 45396 数据安全技术 政务数据处理安全要求
GB/T 45502 服务机器人信息安全通用要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能机器人 intelligent robot

具有环境感知能力与对外交互能力，利用人工智能技术进行学习、推理和决策，并通过执行器自主或在人类指导下执行任务，以完成特定目标的机器系统或物理机器人。

注：人工智能技术包括但不限于机器学习、智能体、计算机视觉。

3.2

政务辅助智能机器人 government affairs support intelligent robot

辅助履行公共管理职责或者提供公共服务，具备一定人格特征，能半自主或全自主进行感知、决策、交互的智能机器人（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：应用程序编程接口（Application Programming Interface）
APP：应用软件（Application）
CPU：中央处理器（Central Processing Unit）
LVM：视觉语言模型（Vision Language Model）
NLP：自然语言处理（Natural Language Processing）
TPU：张量处理器（Tensor Processing Unit）
TLS：传输层安全性协议（Transport Layer Security）
SSL：安全套接层（Secure Sockets Layer）
VPN：虚拟专用网络（Virtual Private Network）

5 基本要求

5.1 建设基本要求

5.1.1 应适配现有政务信息系统，具备与政务信息系统采用的服务器、网络、存储等硬件设备兼容的能力。

5.1.2 应支持网站、APP、小程序、政务服务大厅终端、电话热线等多种渠道接入。

5.1.3 应充分利用现有政务云、大数据中心等基础设施资源，避免重复建设。

5.1.4 应具备业务模块、新增硬件节点的横向扩展与算法迭代、功能增强的纵向升级能力，应预留技术接口以适配未来政务业务场景变化。

5.2 设施基本要求

5.2.1 基于政务专有云部署，提供弹性计算资源。

注：弹性计算是基于云计算技术实现的计算资源管理模式，允许用户根据业务需求动态调整资源规模。

5.2.2 部署 CPU/TPU 服务器，支撑 NLP 模型训练、语音识别推理等 AI 任务。

5.2.3 政务环境的网络支撑应具备网络隔离和专线接入，其中：

——网络隔离应隔离区分政务内网与政务外网，政务内网处理敏感数据，政务外网公开资讯；

——专线接入应通过 VPN 专线对接各部门业务系统，保障数据传输稳定性。

5.3 应用基本要求

5.3.1 应基于用户问法、反馈和人工处理结果，不断优化模型和知识库，实现自我迭代升级。

5.3.2 智能机器人的行为需在预设的、合规的框架内进行，所有交互操作应全程留痕、可追溯，满足监管审计要求。

5.3.3 交互功能应符合政务用户使用习惯，对个人用户提供简洁易懂的操作界面，对政务工作人员提供高效的管理与运维工具。

5.3.4 信息安全应符合 GB/T 45502 的要求。

6 技术架构

6.1 技术参考架构

政务辅助智能机器人技术架构以基础设施层为底座，通过数据资源层提供数据支撑，由技术能力层进行信息感知认知、任务执行和决策，实现与应用服务的衔接，并通过前端交互层面向用户提供服务。全过程提供本地化部署、身份认证、数据加密、监护人制度等安全保障。政务辅助智能机器人技术参考架构见图1。其中：

——基础设施层提供计算、存储、网络安全和其他软硬件基础设施，应保障网络互通、终端兼容，满足跨层级、跨地域政务服务运行需求和系统运行提供基础条件；

——数据资源层为政务辅助智能机器人系统提供内部和外部数据源支撑，以及数据服务、数据存储、数据安全等相关技术资源支撑；

——技术能力层包括感知层、认知层、执行层、决策层；

——前端交互层包括智能机器人、系统原生 UI 界面、智能体对话交互窗口、多模态输入输出处理模块。

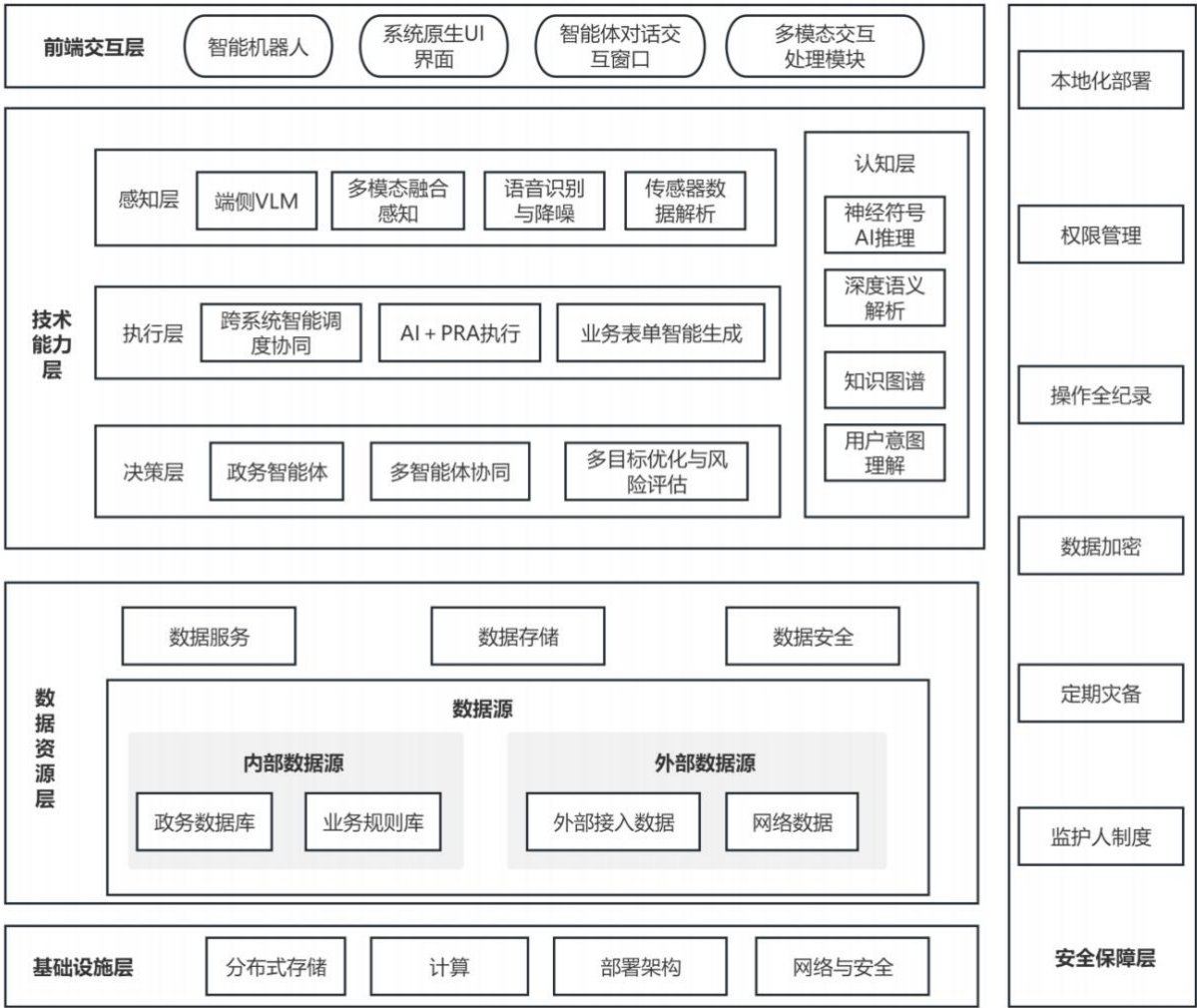


图 1 政务辅助智能机器人技术参考架构

6.2 部署要求

6.2.1 准入审核

政务辅助智能机器人上线部署的准入审核要求如下：

- 主体资质审核，审核建设主体营业资质、信创适配资质、政务项目服务资历，无资质、存在网络安全违法前科企业产品不应进入政务内网；
- 技术能力审核，机器人的软件、硬件和性能需满足具体政务场景的技术服务需求；
- 伦理合规审核，机器人的行为应符合社会道德和法律法规。

6.2.2 部署模式

政务辅助智能机器人的部署应符合GB/T 45301的要求，部署模式主要包括本地化部署、私有云部署和混合云部署。

- 本地化部署，将管理系统、业务引擎、数据库等全部部署在政府自有的机房或指定的私有化环境中，机器人终端通过政务内网/专网与服务器通信；
- 私有云部署，利用政府构建的资源隔离的“政务云”资源池进行部署；
- 混合云部署，同时使用本地化部署和私有云两种模式，并在其间进行安全的数据同步和任务分配。

7 技术能力要求

7.1 感知能力

感知层支持政务场景多模态信息的采集、接入与预处理。集成端侧VLM、语音识别等功能技术，实现视觉信息实时解析，结合多模态融合感知技术对数据进行清洗、格式转换、特征提取，输出可识别、可用的政务数据。

注：多模态信息包括但不限于文本、语音、图像、视频、传感器数据。

7.2 认知能力

认知层支持对政务数据的理解和推理，形成处理政务的任务指令。集成自然语言处理、知识图谱、机器学习等核心技术，可对信息进行语义理解、知识推理和情境分析，能够理解政务术语、政策法规、业务流程等专业领域知识，关联事务推理问题，定期结合实际政务数据优化理解和推理能力。

7.3 执行能力

执行层支持将识别的任务指令转化为具体的操作行为，包括跨系统联动办事、调用政务系统API、生成业务表单、发送通知消息、控制物理设备等，应具备任务调度、异常处理、结果反馈、全流程可控可追溯等能力。

7.4 决策能力

以政务专属智能体为核心，结合政务业务规则和优化目标，基于执行结果，生成智能决策方案。决策层应支持多目标优化、风险评估、策略规划等功能，能够适应动态变化的政务场景。

8 前端交互要求

前端交互应呈现智能服务的终端形态，需实现多模态交互、多终端适配、组件化开发等技术要求。

——多模态交互应适配不同用户习惯，降低操作门槛，可实现文字、语音、视频交互；

——多终端适配应适配政务场景中常见的PC端、移动端及特殊终端；

——组件化开发应优先选择轻量、易维护的框架，适配政务系统的快速迭代需求。

注1：PC端包括但不限于政务大厅终端、官方网站。

注2：移动端包括但不限于政务APP、小程序。

注3：特殊终端包括但不限于智能机器人、自助服务机。

9 数据资源要求

9.1 数据源

9.1.1 内部数据

内部数据是政府各部门内部产生、拥有和管理的数据资源，包括但不限于业务办理数据、行政审批数据、内部公文、档案。智能机器人调用内部数据应满足以下要求。

——访问数据库或内部系统应申请和使用专属身份账号；

——获取数据应通过政务数据共享交换平台或统一的API接口网关；

——开发测试环境与生产环境所用数据应实现逻辑隔离；

——智能机器人的访问策略应与数据级别对应；

——智能机器人进行模型训练、数据分析或对外交互时，应对涉及的敏感个人信息、商业秘密等数据进行隐藏、替换或匿名化等脱敏处理。

9.1.2 外部数据

外部数据是政府系统外部产生的、对政务服务有补充和增强作用的数据资源，包括但不限于其他单位共享数据、公共数据开放平台数据、互联网公开数据，以及由合法商业机构提供的第三方数据。智能机器人调用外部数据应满足以下要求：

——应建立外部数据准入审批机制，组织相关人员审批，评估采集的外部数据的合法性、必要性及安全性；

- 使用外部数据生成报告或提供辅助决策，应明确标注数据来源，保障结果的可解释性和可追溯性；
- 使用外部数据生成报告或提供辅助决策，应将外部数据与内部权威数据进行交叉验证，保障结果的真实性和适用性；
- 外部数据存在使用期限和授权范围的限制要求。应建立管理台账，定期清理超期或不再使用的数据。

9.2 数据存储

9.2.1 结构化数据库

应存储用户办件记录、政务事项清单、业务规则等。

9.2.2 非结构化数据库

应存储政策文档、表单模板、语音录音等。

9.2.3 知识图谱库

应构建政务领域知识网络，包括事项、材料、流程、部门的关联关系，支撑深度问答与逻辑推理。

9.3 数据服务

应提供符合GB/T 45502的L5等级要求的数据接口，采用统一的输入输出格式、调用频率限制、身份认证方式等技术要求。

9.4 数据治理

9.4.1 建立机制

建立常态化数据治理机制，明确岗位职责、治理流程与管控规则，动态迭代治理标准与质量规则。定期开展数据风险扫描、合规复盘，对废弃交互日志、过期训练数据集按规范流程销毁，留存处置台账。

9.4.2 分级分类

政务数据应按照GB/T 43697的要求进行分类分级管控，区分知识库静态数据、动态交互数据，模型生成数据分类存储加密，具体要求如下：

- 核心、重要数据执行原始数据不出域，进行物理隔离；
- 自然人身份、联系方式、地址、证照号等字段进行脱敏、屏蔽、去标识化；
- 机器人对外答复输出前应过滤敏感字段，不应将原始隐私数据直接返回用户。

9.4.3 全生命周期管理

机器人数据接入、模型训练、用户交互、内容输出、日志存储、归档销毁全程链路标识留痕，动态更新。

9.5 数据安全

9.5.1 安全保护

应制定数据安全保护机制，数据传输过程中应采用加密算法、建立安全通道、访问控制、权限设置等方式保护数据安全，安全技术防护应符合GB/T 45396的要求。

9.5.2 数据加密

9.5.2.1 政务辅助智能机器人处理、存储、传输的所有政务数据，应采用符合国家密码管理标准的加密算法进行加密保护，确保数据全生命周期的保密性。

9.5.2.2 数据传输过程应采用SSL/TLS等安全协议进行加密，防止数据在传输过程中被窃听、篡改或泄露。

9.5.2.3 敏感政务数据（如公民个人信息、涉密业务数据）应采用高强度加密算法进行存储加密，密钥管理应符合国家密码管理相关规定，建立密钥生成、存储、分发、销毁的全流程管控机制。

10 安全保障要求

10.1 权限管理

10.1.1 应建立分级分类的用户身份管理体系，对政务工作人员、运维人员、第三方人员等不同角色实施差异化的身份认证与权限管控。

10.1.2 采用多因素认证方式，结合账号密码、数字证书、生物识别等技术，保障用户身份的真实性与唯一性，防止非法用户接入系统。

10.1.3 应实现权限的最小化配置，用户仅能访问其职责范围内的功能与数据，不应超权限访问、修改或删除政务敏感信息。

10.1.4 定期开展用户身份核查与权限审计，及时清理离职、调岗人员的账号权限，防止权限滥用。

10.2 操作全记录

10.2.1 应对政务辅助智能机器人的所有用户操作、系统行为、数据交互过程进行全程日志记录，日志内容应包括操作主体、操作时间、操作内容、操作结果及 IP 地址等关键信息。

10.2.2 日志记录应具备不可篡改、不可删除的特性，存储周期不应低于国家及地方政务信息系统日志留存的相关规定。

10.2.3 应建立日志审计机制，定期对操作日志进行分析核查，及时发现并处置异常操作、违规访问等安全事件，审计记录需留存备查。

10.2.4 操作、问答、导出全链路日志留存不少于 6 个月。

10.3 定期灾备

10.3.1 应建立政务辅助智能机器人数据备份与灾难恢复机制，制定完善的灾备方案，明确备份策略、恢复流程与责任分工。

10.3.2 按照既定周期对系统配置文件、业务数据、日志记录等进行全量备份与增量备份，备份数据应存储于异地安全存储介质中，防止单点故障导致数据丢失。

10.3.3 定期开展灾备演练与恢复测试，验证备份数据的完整性与可用性，确保在发生系统故障、数据损坏等突发事件时，能够快速恢复业务运行，降低安全风险。

10.4 监护人制度

10.4.1 应建立政务辅助智能机器人安全监护人制度，明确监护人的职责权限，监护人由政务部门指定的具备相关资质的工作人员担任。

10.4.2 监护人负责监督智能机器人的运行状态、业务操作与数据交互过程，对机器人输出的敏感信息、决策建议等内容进行审核确认，防止违规输出或不当处置政务业务。

10.4.3 建立监护人履职记录机制，对监护人的审核操作、监督行为、处置结果等进行记录归档，定期开展履职情况核查，确保监护人制度有效落地。

11 风险控制

11.1 监测预警

实时监测风险，建立风险模型，对风险进行量化评分和动态定级，7×24小时自动扫描风险监测任务清单，对存在超期风险的任务自动预警。

11.2 应急保障

11.2.1 应建立常态化应急保障长效机制，制定专项应急预案，实现 7×24 小时全流程值守。

11.2.2 识别风险后可自动启动预设处置流程，系统将预警和处置指令直接推送至一线处置人员。

11.2.3 应急保障覆盖包括但不限于操作运行、数据安全、网络联动，内容如下：

——运行保障，建立分级处置机制，依托冗余算力、备用知识库实现服务降级与快速恢复，及时处置卡顿、宕机等问题，留存故障处置台账；

——数据安全保障，针对数据泄露、越权调取、敏感信息外发等突发事件，立即切断交互通道、冻结权限、溯源排查，依托数据备份完成恢复整改；

——网络联动保障，针对网络攻击、接口断连等情况，启动接口熔断、流量清洗和网络隔离措施。

11.3 持续改进

分析处置结果，梳理漏判、误判点，结合处置结果自动标记、更新风险点位，持续优化调整政务辅助智能机器人的安全策略、技术架构。

参 考 文 献

- [1] 中央网信办、国家发展和改革委员会. 政务领域人工智能大模型部署应用指引. 2025年
 - [2] 国家网信办、国家发展改革委、工业和信息化部. 智能体规范应用与创新发展实施意见. 2026年
-