人工智能（AI）办公秘书应用规范

编制说明

《人工智能（AI）办公秘书应用规范》标准编制组

2026 年 11 月

一、工作简况

（一）任务来源

为规范地市级党政机关个人岗位人工智能办公辅助应用，明确人工智能办公秘书的能力边界、人机协同关系与安全合规要求，梅州市政务大数据管理中心于 2026 年 9 月提出《人工智能（AI）办公秘书应用规范》团体标准立项申请，由广东省数字政务协会批准立项。本标准与《人工智能（AI）协同管理规范》为配套文件：本标准面向个人岗位的办公辅助应用，《人工智能（AI）协同管理规范》面向跨部门、跨层级的组织协同管理，两者适用范围互不重叠、要求相互衔接。

（二）起草单位

本标准由梅州市政务大数据管理中心提出，广东省数字政务协会归口。依据立项申请书，主要起草单位为梅州市政务大数据管理中心、广州市数字政务运营中心、江门市大数据管理中心，项目负责人为徐雄鹰。编制组由政务管理部门、技术支撑单位与平台应用单位的专业人员组成，具体成员名单及分工待编制组确认后在标准前言中补充。

（三）目的和意义

国家政策层面，国务院《关于深入实施“人工智能+”行动的意见》提出新一代智能终端、智能体应用普及率目标，《政务领域人工智能大模型部署应用指引》将“机关办公”列为典型应用场景，为机关办公场景的人工智能规模化应用提供了政策依据。省级层面，广东省《加快数字政府领域通用人工智能应用工作方案》（粤政数〔2023〕

41 号）推动政务大模型体系建设，省级政务人工智能一体化体系及“粤政易”智能助手已在部分省直单位试点，并同步出台认证体系、接口标准、知识库建设、算力运营、安全分级等标准规范；但面向岗位、面向具体办公场景的“AI 秘书”应用规范仍属空白。

地市实践层面，梅州市已于 2025 年 3 月完成 DeepSeek R1 全尺寸模型在一体化政务协同办公平台的本地化部署，在 PC 端与“粤政易”移动端同步上线智能助手，覆盖公文起草、智能校对、会议纪要生成等场景。现有实践多集中于“文档处理”单点能力，公文拟办、会议安排、信息推送、智能提醒等拟人化秘书工作流尚无统一规范，人工智能“辅助型”定位边界、拟办越权风险、涉密数据防泄露、模型幻觉防控等安全要点缺乏本地化约束依据。

本标准旨在建立三个层面的统一：在定位层面，明确人工智能办公秘书为使用者履职的辅助工具，不改变岗位职责与法定职责，不替代使用者作出决策；在能力层面，规定信息获取与整理、文档起草与辅助写作、会务辅助、待办与日程管理、知识沉淀与复用、事务跟办与提醒六个能力域的完整链路与人工确认要求；在安全层面，规定数据分类分级、最小授权、过程留痕、保密禁限、生成内容标识与生成式人工智能服务合规要求。本标准的实施有助于在不转移责任主体的前提下提升个人岗位办公效率，并为地市级政务人工智能办公辅助应用提供可执行、可追溯的依据。

本标准属于推荐性团体标准，不设定强制性要求；涉及提醒阈值、评价指标基线、记录保存期限等具体数值，均以参数化或“不宜少于”

方式表述，由使用单位结合本地实际确定。

（四）编制原则

本标准制定遵循以下原则:

1. 协调性

本标准遵循国家有关标准化、网络安全、数据安全、个人信息保护和保守国家秘密的法律法规要求，与党政机关公文格式、电子公文系列标准、信息技术服务运行维护、人工智能大模型及安全类现行国家标准保持协调，并与《人工智能（AI）协同管理规范》在适用范围、主体设置、智能体术语定义上保持一致。行政法规、部门规章和地方政策文件不列入规范性引用文件，改列入参考文献，以符合 GB/T 1.1—2020 对规范性引用文件范围的要求。

2. 实用性

本标准立足地市级党政机关文秘、综合办公等个人岗位的日常办公事务，条款与现有办公自动化系统、公文系统和知识库的技术条件相适应。附录以资料性样表形式给出能力清单、提示词要素与人工复核要点，供使用单位按岗位实际增删；具体阈值、评价指标与基线值由使用单位自行设定，不作统一强制值。

3. 规范性

本标准按照 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》确立的规则编写，章节划分、条标题、列项引导语、术语条目、注、资料性附录与参考文献的设置均符合该导则要求；第 2 章仅列经正文规范性引用、构成本文件必不可少条

款的现行国家标准。

4. 安全性

个人岗位办公事务涉及公文凭据、敏感数据和个人信息，本标准将安全管理要求作为独立章（第 8 章）设置，并在第 7 章人机协同要求中明确辅助执行边界、强制人工确认环节与禁止事项，坚持“辅助不越位、人在回路、过程留痕”，实现发展与安全并重。

（五）编制过程

（1）标准立项。2026 年 9 月 14 日，经梅州市政务大数据管理中心提出立项申请，广东省数字政务协会审批后发布立项公告。

（2）成立编制组。2026 年 10 月 9 日，立项后组建标准编制组，由政务管理部门与平台应用单位专业人员组成，负责标准文本起草与调研验证。

（3）调研与起草。编制组围绕梅州市一体化政务协同办公平台智能助手的本地化部署与试运行情况开展调研，梳理信息处理、文档办理、会务组织、事务跟办等个人岗位办公事务流程，形成标准框架与章节划分草案，完成标准初稿。

（4）适用范围收敛与内部审议。编制组对初稿进行内部审议，重点审议与《人工智能（AI）协同管理规范》的适用边界、规范性引用文件范围、术语定义的技术来源以及量化阈值的表述方式，形成修改意见，编制组修改后形成征求意见稿。

二、标准的主要内容

（一）技术内容说明

本标准规定了面向个人岗位的人工智能办公秘书应用的总体要求、能力要求、人机协同要求、安全管理要求和运行与评价要求，适用于地市级党政机关及其下属事业单位的文秘、综合办公等个人岗位，在日常办公事务中借助人工智能完成信息处理、文档办理、会务组织、事务跟办等工作。本标准不适用于跨部门、跨层级政务协同工作中的人工智能管理，该部分内容见《人工智能（AI）协同管理规范》；本标准不改变国家有关党政机关公文处理、政务信息共享、保守国家秘密、个人信息保护及生成式人工智能服务管理的规定。

本标准的主要技术内容包括:

规范性引用文件: 列出现行国家标准 14 项，涵盖党政机关公文格式、质量管理体系、网络安全等级保护、信息技术服务运行维护、党政机关电子公文格式与接口、系统建设、个人信息安全、数据安全能力成熟度、密码应用、人工智能大模型通用要求与评测指标、生成式人工智能服务安全基本要求、人工智能风险管理能力评估，均为正文规范性引用、构成本文件必不可少的条款。行政法规、部门规章与地方管理文件改列入参考文献。

术语和定义: 界定办公秘书、人机协同、辅助执行、待办与提醒、知识库、智能体等 6 个术语。各术语均在注中说明技术来源或形成方式，详见本章“术语的来源与确定依据”。

缩略语: 给出 AI、KPI、OA、PDCA、RAG 等 5 个缩略语。

总体要求（第 5 章）：提出辅助不越位、权责清晰、人在回路、安全合规、持续改进五项基本原则；建立含信息获取与整理、文档起草与辅助写作、会务辅助、待办与日程管理、知识沉淀与复用、事务跟办与提醒六个能力域的能力总体框架并给出框架图；明确使用者、使用单位、技术支撑方三类主体及其职责，明确本文件不设督办方；提出模型与智能体服务、知识库管理、接口集成、数据治理四项技术要求。

能力要求（第 6 章）：按六个能力域分别规定信息检索、要点提取、材料归集；提纲拟写、段落起草、文字润色、格式套用；议题征集、日程协调与通知拟发、记录转写与纪要生成、待办拆解与派发；待办生成、时限提醒、优先级排序；经验总结、知识检索与引用；任务跟踪、台账填报辅助等能力项，并规定输出可追溯、来源标注与人工确认要求。

人机协同要求（第 7 章）：规定辅助执行边界、授权清单与强制人工确认环节，列明涉及法定职责、涉密信息、对外正式行文、个人权益处置、资金拨付与项目评审结论等不得由人工智能代为处置的事项，规定过程可追溯要求，以及禁止代为决策、禁止自动对外发送、禁止处理的数据类型、禁止无人值守运行四类禁止与限制事项。

安全管理要求（第 8 章）：规定数据安全与保密、权限与审计、内容可信与标识、生成式人工智能服务合规四方面要求，落实可输入、限输入、禁输入数据分类规则，数据不出域、密码应用、生成内容标识以及输入内容—模型版本—生成结果—人工处置的记录链。

运行与评价（第 9 章）：规定部署与接入、培训与使用规范、使用效能评价、持续改进要求，明确评价指标与基线值由使用单位自行确定，并区分“效率提升”与“责任转移”两种情形。

附录 A（资料性）人工智能办公秘书应用能力清单样表：按能力域列出 18 项能力的典型输出、人工确认要求与建议授权方式，作为使用单位编制授权清单的参考格式。

附录 B（资料性）典型提示词与人工复核要点示例：给出要点提取、提纲拟写、段落起草、文字润色、纪要生成、台账填报等场景的提示词要素、人工复核要点与常见风险，说明“不确定时标注存疑”“仅归纳已明确表述的内容”等限定语对抑制模型编造内容的作用。

附录 C（资料性）与《人工智能（AI）协同管理规范》的衔接关系：从适用对象、管理范围、主体设置、处理方式、责任承担、章节对应与不适用范围等方面给出对照表，说明两份文件的配套关系。

（二）术语的来源与确定依据

本标准第 3 章界定的 6 个术语均非现行国家标准已界定的同名术语，其定义系在本标准技术内容范围内形成。形成方式可归为三类：一是将现行国家标准中的相关要素按个人岗位办公场景重新组合形成新的组合概念；二是参照现行国家标准中某项要素的功能内涵加以限定后形成；三是参照现行技术文件中的定义并结合本标准的适用边界加以限定。各术语的来源与转化依据如下：

办公秘书（3.1）：组合形成。参照 GB/T 45288.1—2025《人工智能 大模型 第 1 部分：通用要求》中“大模型”的技术内涵，结

合文秘、综合办公岗位在信息处理、文档办理、会务组织、事务跟办等方面的功能定位组合形成。该术语为本文件提出，用于界定规范对象为岗位级应用形态，而非平台或系统。

人机协同（3.2）：转化形成。以人工智能输出的使用方式为划分依据，将“人工智能提供辅助”与“人工智能独立完成处置动作”两种方式并列，并明确由使用者决定采用何种方式。其可控性要素参照 GB/T 45288.1—2025 中人工智能应用可控性相关要求形成，本术语在此基础上补充“使用者决定”这一责任主体要素。

辅助执行（3.3）：自主提出。为区分人工智能的辅助性处置与依据授权独立实施的处置行为而设定，明确处置动作须限定在使用者确认或授权范围内、且不单独产生对外效力。该术语是第 7 章辅助执行边界与强制人工确认条款的概念基础。

待办与提醒（3.4）：参照形成。参照 GB/T 28827.1—2022《信息技术服务 运行维护 第 1 部分：通用要求》中服务内容的组织方式形成，界定为依据事项办理状态、办理时限或预设规则自动生成并推送给使用者的提示信息；具体阈值与推送方式在注中明确由使用单位自行设定，本文件不作统一规定。

知识库（3.5）：参照形成。参照 GB/T 33482—2016《党政机关电子公文系统建设规范》中电子公文标准化套件的组成思路形成，界定为汇集本岗位业务文件、制度规定、历史案例等资料、支持检索引用与更新的资源集合，并在第 5.4.2 条与第 6.5 章中规定其来源、按权限检索与定期更新要求。

智能体（3.6）：参照现行技术文件定义。参照全国网络安全标准化技术委员会《人工智能安全治理框架》2.0 中“智能体（agent）”的定义，并与《人工智能（AI）协同管理规范》保持一致。需说明的是，GB/T 45288.1—2025 未界定智能体术语；智能体互联相关标准尚在发展之中，本文件涉及接口衔接的条款均以“兼容协议的选择宜以正式发布文本为准”表述，避免引用尚未定稿的编号。

关于自主术语的合规性说明：本文件自主形成的术语遵循三项原则：一是所界定对象在现行国家标准中无同名术语，不存在定义冲突；二是术语所含要素均可在现行国家标准或技术文件中找到出处，并已在注中说明，不引入无法溯源的概念；三是术语的适用边界在定义中予以限定，避免超出现行制度安排的解释空间。“人在回路”“辅助不越位”等通用概念或原则名称不作为术语收录，仅在第 5.1 条基本原则中使用，其内容由第 7 章各条款具体体现。

（三）主要量化指标与阈值的设定

本文件以“可设定、可考核、不作统一强制值”为原则处理数值型要求：正文只规定指标项目、评价维度与责任主体，具体阈值和基线值由使用单位结合岗位实际确定。主要处理如下：

提醒阈值与推送方式：第 6.4 条规定提醒阈值由使用单位按事项类别分别设定，本文件不作统一强制值；提醒渠道宜结合本地实际确定。此类数值与地市办公节奏、事项紧急程度分布相关，统一规定将脱离实际。

评价指标与基线值：第 9.3 条规定从信息处理效率、文档质量、

会务组织效率、待办履约率、用户满意度等维度开展评价，指标设定方法参照 GB/T 33850，具体指标与基线值由使用单位自行确定，并明确不应以人工智能输出量替代对文档质量的评价。

记录保存期限：第 7.4 条与第 8.4 条规定处理记录与记录链保存期限“不宜少于 1 年”，该数值依据国家关于生成式人工智能服务管理的规定及安全审计的一般实践提出，采用“不宜少于”的推荐性表述，具体期限由使用单位根据管理需要确定。

资料性附录中的示例内容：附录 A 能力清单与附录 B 提示词要素均为资料性示例，不含强制数值，用于说明条款的适用形式，不构成对使用方的强制要求。

三、知识产权情况说明

本标准不涉及知识产权，与立项申请书“本文不涉及知识产权问题”的说明一致。

四、与现行相关法律、法规和强制性国家标准的关系

本标准与现行法律、法规和强制性国家标准均不存在冲突。

本标准的制定遵循《中华人民共和国标准化法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国保守国家秘密法》《中华人民共和国密码法》的相关规定，并在第 8 章安全管理中具体落实网络安全等级保护、个人信息保护、数据分类分级、商用密码应用等要求。第 1 章明确本文件不改变国家有关党政机关公文处理、政务信息共享、保守国家秘密、个人信息保护及生成式人工智能服务管理的规定。

本标准不设定强制性条款，不替代、不抵触现有强制性国家标准。所引用的国家标准均为现行推荐性标准；涉及生成式人工智能的合规要求，与《生成式人工智能服务管理暂行办法》的管理要求相衔接——本标准通过自述要求的方式落实算法备案选用、生成内容标识、记录链保存等义务，不直接引用部门规章文号。

关于引用文件范围的说明：本标准第 2 章仅列出现行 GB / GB/T 推荐性国家标准。行政法规、部门规章和地方管理文件不列入规范性引用文件，依据是 GB/T 1.1—2020 关于被规范性引用的文件应为标准化文件、不得规范性引用法律、行政法规、规章和其他政策性文件的规定。此类文件已列入参考文献，供读者了解政策来源。

五、相关国内标准情况简要说明

与本标准较为相关的标准规范包括：

GB/T 9704—2012《党政机关公文格式》与 GB/T 33476、GB/T 33479、GB/T 33482 等党政机关电子公文系列标准，分别规定公文格式要素、电子公文格式、交换接口与系统建设要求，本标准在提纲拟写、格式套用、接口集成等条款中引用上述标准，以保持公文处理环节的格式与接口一致。

GB/T 22239—2019、GB/T 35273—2020、GB/T 37988—2019、GB/T 39786—2021、GB/T 45654—2025 等安全类标准，分别规定网络安全等级保护、个人信息安全、数据安全能力成熟度、密码应用与生成式人工智能服务安全基本要求，本标准第 8 章据此落地数据分类分级、权限审计、内容标识与合规要求。

GB/T 45288.1—2025、GB/T 45288.2—2025《人工智能 大模型》系列标准与 GB/T 46347—2025《人工智能 风险管理能力评估》，分别规定大模型通用要求、生成内容质量评测指标与方法、风险管理能力评估方法，本标准在模型与智能体服务、纪要生成、内容可信等条款中引用；GB/T 19001—2016、GB/T 28827.1—2022 分别在持续改进、运维服务能力与培训使用规范等条款中引用。

立项阶段检索到的相近标准包括《高校行政人员 AI 技术辅助办公通用要求》（T/JXEA 067—2025）、《信息技术 人工智能 智能助理能力等级评估》（T/CESA 1038—2019）、《AI 无界办公管理平台技术规范》（T/UNP 54—2026）、《人工智能关键技术 办公大模型系统技术要求》（SJ/T 12114—2025），以及 GB/T 45654—2025、GB 45438—2025 等通用安全与标识标准。上述标准分别面向高校行政群体、全行业智能助理能力分级、平台技术架构与上游技术框架，未专门针对地市级政务个人岗位“AI 秘书”的应用场景、服务流程、人机边界与安全合规进行系统规定。

本标准侧重岗位级应用的能力边界、人机协同与安全管理要求，而非平台架构或模型技术实现，与上述标准在各自领域内互补，不构成替代关系。经检索，目前尚未见专门针对地市级政务个人岗位人工智能办公秘书应用的国家标准、行业标准或团体标准，本标准填补了“省级政务智能底座—岗位应用场景”之间的应用层空白。

六、重大分歧意见的处理经过和依据

编制过程中，编制组对部分技术内容进行了充分讨论并达成一致，

主要包括:

一是关于适用范围与配套标准的关系。立项申请书曾将适用范围设想为一体化协同办公平台中 AI 秘书的设计、部署、运营与评估，并包含“待办与督办提醒”等能力。经审议，为避免与《人工智能（AI）协同管理规范》在跨部门、跨层级协同管理事项上重叠，最终将本文件收敛为面向个人岗位的办公辅助应用，平台部署与接入要求仅在第 9.1 条作衔接性规定；涉及事项跟踪、预警与督办的，按配套标准执行，本文件跟踪结果仅供使用者了解情况、不得作为督办依据。

二是关于主体设置。经讨论确认个人岗位应用不存在督办关系，本文件只设使用者、使用单位、技术支撑方三类主体，不设督办方；配套标准面向组织间协同，设管理方、使用方、服务方、督办方四类主体。两者的差异已在附录 C 中列表说明。

三是关于具体阈值是否统一规定。讨论后确定正文不设统一强制值，提醒阈值、评价指标与基线值以参数化方式由使用单位设定，记录保存期限采用“不宜少于 1 年”的推荐性表述。

四是关于规范性引用文件范围。依据 GB/T 1.1—2020 的要求，第 2 章仅列现行国家标准，行政法规、部门规章与地方管理文件改列参考文献，相关义务以自述要求方式在条款中落地，不直接引用规章文号。

五是关于术语章收录范围。讨论后决定仅收录本文件特有、且在正文条款中实际引用的概念；“人在回路”“辅助不越位”等通用概念或原则名称不作为术语收录，其内容在第 5.1 条与第 7 章具体体

现。

六是关于生成式人工智能服务合规的表述方式。讨论后确定以自述要求方式落实算法备案选用、生成内容标识与记录链保存义务，同时在第 8.4 条明确本文件不改变国家有关生成式人工智能服务管理的规定，避免与现行规章形成引用冲突。

七、标准性质的建议

本标准作为推荐性标准，属于团体标准，供协会会员和社会自愿采用。

八、标准实施建议

本标准批准发布实施后，尽快将批准信息通告编制小组成员单位及其他有关单位，积极组织宣传与培训，使地市级党政机关文秘、综合办公岗位的使用者，以及管理、业务、技术人员准确理解人工智能办公秘书的能力边界、授权范围、禁止事项与人工确认要求。

建议在已具备一体化政务协同办公平台与本地化大模型部署基础的地市先行开展试点，重点验证授权清单的编制方法、提醒阈值的参数化配置、附录 A 能力清单样表与附录 B 提示词复核要点的适用性，试点结果用于后续修订完善。

建议与《人工智能（AI）协同管理规范》配套宣贯、同步实施，避免两套文件在适用范围与主体职责上产生理解偏差；鼓励使用单位将执行情况与发现的问题及时反馈至归口团体或起草单位，为标准完善做好准备。

九、其他应说明的事项

本标准与配套标准的关系：本标准与《人工智能（AI）协同管理规范》为配套文件，分别规范个人岗位应用与组织协同管理中的人工智能应用，两者适用范围互不重叠、要求相互衔接。两份文件的“智能体”术语定义一致，第 5 章总体要求与第 5.4 条技术要求结构对应，第 8.4 条与配套标准相应条款在生成式人工智能服务合规要求上保持一致。

关于标准文本的待补充事项：征求意见稿前言中的起草单位、主要起草人目前为“【待补充】”占位，封面标准编号、发布日期与实施日期亦为占位；上述信息应在形成送审稿前依据编制组成立文件与归口单位立项公告补齐。本编制说明所载起草单位依据立项申请书列示，最终以标准前言为准。

本编制说明与征求意见稿同步编写，后续如根据征求意见处理结果调整技术内容，应同步修订本说明相应章节。