ICS 35.240
CCS L73

团　　体　　标　　准

T/DGAG XXX—2026

人工智能（AI）办公秘书应用规范

Specification for artificial intelligence (AI) office secretary application

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

广东省数字政务协会　　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 缩略语 2
5 总体要求 2
5.1 基本原则 2
5.2 能力总体框架 2
5.3 使用者与职责 3
5.4 技术要求 3
6 能力要求 4
6.1 信息获取与整理 4
6.2 文档起草与辅助写作 4
6.3 会务辅助 5
6.4 待办与日程管理 5
6.5 知识沉淀与复用 5
6.6 事务跟办与提醒 6
7 人机协同要求 6
7.1 辅助执行边界 6
7.2 人工确认环节 6
7.3 不得代为处置事项 6
7.4 过程可追溯 7
7.5 禁止与限制事项 7
8 安全管理要求 7
8.1 数据安全与保密 7
8.2 权限与审计 7
8.3 内容可信与标识 8
8.4 生成式人工智能服务合规 8
9 运行与评价 8
9.1 部署与接入 8
9.2 培训与使用规范 8
9.3 使用效能评价 8
9.4 持续改进 8
附录 A　（资料性）　人工智能办公秘书应用能力清单样表 10
附录 B　（资料性）　典型提示词与人工复核要点示例 11
参考文献 12

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。

本文件由梅州市政务大数据管理中心提出。

本文件由广东省数字政务协会归口。

本文件起草单位：。

本文件主要起草人：

人工智能（AI）办公秘书应用规范

1 范围

本文件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。

本文件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，在基于协同办公平台的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。

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 9704—2012 党政机关公文格式

GB/T 19001—2016 质量管理体系 要求

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 28827.1—2022 信息技术服务 运行维护 第 1 部分：通用要求

GB/T 33476（所有部分） 党政机关电子公文格式规范

GB/T 33479—2016 党政机关电子公文交换接口规范

GB/T 33482—2016 党政机关电子公文系统建设规范

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GB/T 45288.1—2025 人工智能 大模型 第 1 部分：通用要求

GB/T 45288.2—2025 人工智能 大模型 第 2 部分：评测指标与方法

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

3 术语和定义

下列术语和定义适用于本文件。

3.1

办公秘书 office secretary

以人工智能技术辅助个人岗位完成信息处理、文档办理、会务组织、事务跟办等日常办公事务的应用形态。

注：本术语系本文件提出，参照 GB/T 45288.1—2025 中“大模型”的技术内涵与日常办公场景中辅助性岗位的功能定位组合形成。

3.2

人机协同 human-AI collaboration

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，由使用者决定采用何种方式的协同工作方式。

注：本术语系本文件提出，人工智能部分参照 GB/T 45288.1—2025 中人工智能应用可控性相关要求形成。

3.3

辅助执行 assistive execution

人工智能在使用者确认或授权范围内完成的处置动作，该动作不单独产生对外效力。

注：本术语系本文件提出，用于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。

3.4

待办与提醒 to-do and reminder

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。

注：参照 GB/T 28827.1—2022 中服务内容的组织方式形成，具体阈值由使用单位自行设定。

3.5

知识库 knowledge base

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。

注：参照 GB/T 33482—2016 中电子公文标准化套件的组成思路形成。

3.6

智能体 agent

具备自主感知、规划与工具调用能力的人工智能软件实体。

注：本术语定义与《人工智能（AI）协同管理规范》一致，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”的定义形成。GB/T 45288.1—2025 未界定智能体术语。智能体互联相关标准处于发展之中，编号与状态以正式发布文本为准。

4 缩略语

下列缩略语适用于本文件。

AI：人工智能（artificial intelligence）

KPI：关键绩效指标（key performance indicator）

OA：办公自动化（office automation）

PDCA：策划—实施—检查—处置（plan-do-check-act）

RAG：检索增强生成（retrieval-augmented generation）

5 总体要求

5.1 基本原则

人工智能办公秘书应用应遵循下列原则：

a) 辅助不越位：人工智能的功能定位为使用者履职的辅助工具，不改变使用者的岗位职责与法定职责，不替代使用者作出决策；

b) 权责清晰：使用单位应明确使用者的岗位职责与人工智能能力的授权范围，人工智能辅助执行产生的后果由授权人承担；

c) 人在回路：涉及发文、呈批、涉密处置、资金拨付等关键环节的，应保留人工确认与复核，不得由人工智能独立处理；

d) 安全合规：应用全过程应落实数据分类分级、最小授权、过程留痕、保密禁限与生成内容标识要求；

e) 持续改进：应基于使用效能评价与反馈结果，迭代优化知识库、规则与能力配置。

5.2 能力总体框架

人工智能办公秘书应用的能力总体框架应符合下列要求：

a) 能力构成宜包括信息获取与整理、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方面；

b) 各能力域应形成从信息输入到处置动作输出的完整链路，输出内容应可追溯至输入来源；

c) 人工智能能力的启用范围应由使用单位按岗位实际确定，并经使用者确认后生效；

d) 各能力域的技术实现宜统一依托同一人工智能服务与知识库，避免形成相互割裂的多套系统。

人工智能办公秘书应用能力总体框架图见图1。

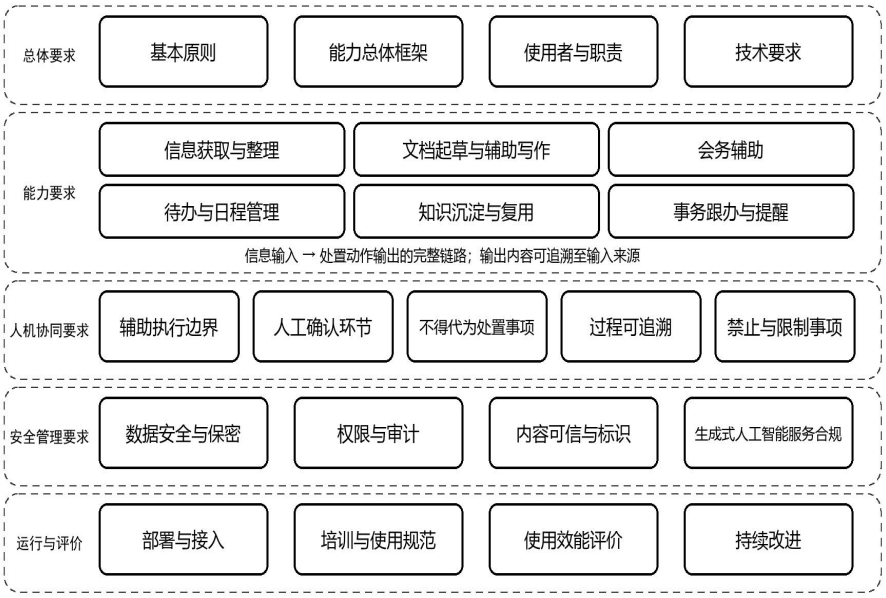


图 1　人工智能办公秘书应用能力总体框架

5.3　使用者与职责

人工智能办公秘书应用应明确下列参与者及其职责：

a)　使用者：提出业务需求、确认人工智能输出、承担处置责任；

b)　使用单位：确定授权范围、落实安全合规要求、组织使用培训、开展效能评价；

c)　技术支撑方：负责人工智能服务的建设、部署、运维与技术支持，保障服务可用性与数据安全。

本文件不设置督办方。跨部门、跨层级协同事项的跟踪、预警与督办，按《人工智能（AI）协同管理规范》执行。

注：与《人工智能（AI）协同管理规范》5.3 的差异在于：该文件面向组织间协同，设管理方、使用方、服务方、督办方四类主体；本文件面向个人岗位，不存在督办关系，故不设督办方。

5.4　技术要求

5.4.1　模型与智能体服务

模型与智能体服务的选用与权限控制应符合下列要求：

a)　人工智能大模型的通用要求宜符合 GB/T 45288.1 的规定；

b)　宜支持多模型接入与国产化部署，模型调用应可审计、可追溯；

c)　智能体的工具调用权限应受使用单位授权范围约束，不得超出授权访问其他数据；

d)　宜预留与上级政务大模型平台的衔接接口，兼容协议的选择宜以正式发布文本为准。

5.4.2　知识库管理

知识库的内容来源、检索引用与更新维护应符合下列要求：

a)　知识库内容应来源于正式发布的制度文件、模板与历史办结材料，来源不明的材料不得纳入；

b)　知识库应支持按权限范围检索与引用，输出内容应标注来源文件名称与生效状态；

c)　知识库应建立定期更新机制，制度修订或文件废止后应及时同步；

d)　涉及个人信息的知识内容应按 GB/T 35273 的规定处理。

5.4.3　接口集成

与既有办公系统的接口集成应符合下列要求：

a)　与办公自动化系统、公文系统、政务邮箱、即时通信平台的对接，应遵循统一的接口定义、鉴权方式与错误码规范；

b)　公文相关接口的具体要求宜符合 GB/T 33476、GB/T 33479、GB/T 33482 的规定，不应另行约定不兼容的协议；

c） 接口调用应记录调用主体、时间、参数与返回结果。

5.4.4 数据治理

人工智能处理数据的分类分级、安全能力与追溯管理应符合下列要求：

a） 人工智能处理的数据应实施分类分级，明确哪些数据可输入、哪些数据仅可本地留存、哪些数据不得输入人工智能服务；
b） 数据安全能力宜符合 GB/T 37988 的规定；
c） 个人信息处理应符合 GB/T 35273 的规定；
d） 服务运行数据应支持追溯，数据安全能力成熟度评估宜从数据治理、模型管理、场景落地、风险控制四个维度开展自评。

6 能力要求

6.1 信息获取与整理

6.1.1 信息检索

信息检索的范围控制与结果标注应符合下列要求：

a） 应支持在授权范围内检索本单位业务文件、制度规定与历史材料；
b） 检索结果应标注来源、发布机关与生效日期，对已废止或失效的文件应明确提示；
c） 不应输出检索范围以外的内容。

6.1.2 要点提取

要点提取应保证结果可回溯至原文，并符合下列要求：

a） 应对指定材料提取办理要点、责任主体、时限要求与关键风险项；
b） 提取结果应可回溯至原文位置，使用者可核对原文；
c） 对材料中表述不清或存在歧义的内容，应标注提示而不应自行推定。

6.1.3 材料归集

材料归集应保持原始材料的真实与完整，并符合下列要求：

a） 应支持按事项、时限、来源等维度归集材料；
b） 归集结果应保持原始文件的形式与内容，不得改写原始材料；
c） 涉密材料的归集与传递应按保密规定执行，不经人工智能服务处理。

6.2 文档起草与辅助写作

6.2.1 提纲拟写

提纲拟写应以使用者输入的要点为依据，并符合下列要求：

a） 应支持依据使用者输入的要点生成文档提纲；
b） 提纲结构宜参照 GB/T 9704 规定的公文格式要素组织；
c） 提纲应经使用者确认后方可进入起草环节。

6.2.2 段落起草

段落起草应以已确认的提纲为边界，并符合下列要求：

a） 应支持按确认的提纲逐段生成初稿；
b） 初稿中的事实、数据、引用条款应可追溯至输入材料或知识库来源；
c） 不应生成涉及政策解释、结论性判断的内容。

6.2.3 文字润色

文字润色应限于语句通顺与用词规范层面，并符合下列要求：

a） 应支持对使用者本人已起草的文字进行语句通顺、用词规范层面的修改；
b） 润色不应改变原意，涉及实质性修改的应提示使用者确认；

c） 法律政策文本、合同文本的实质性修改应由使用者决定。

6.2.4 格式套用

格式套用应依据本单位公文模板，并符合下列要求：

a） 应支持套用本单位公文模板，套用结果宜符合 GB/T 9704 与 GB/T 33476 的规定；

b） 套用后应保留人工确认环节，不应直接进入用印或发文流程。

6.3 会务辅助

6.3.1 议题征集

议题征集与汇总应标明来源信息，并符合下列要求：

a） 应支持向参会人员发起议题征集并汇总反馈；

b） 议题汇总结果应标注提出单位与提出时间。

6.3.2 日程协调与通知拟发

会议日程协调与通知拟发应保留使用者确认环节，并符合下列要求：

a） 应支持依据与会人员可用时间生成候选日程；

b） 会议通知的拟发内容应经使用者确认后方可发送；

c） 会议通知的发送应使用单位指定的渠道。

6.3.3 记录转写与纪要生成

会议记录转写与纪要生成应限定于非涉密会议，并符合下列要求：

a） 应支持会议录音转写与要点提取；

b） 会议纪要的生成内容宜符合 GB/T 45288.2 关于大模型生成内容质量评测的要求，纪要定稿应经使用者审核确认；

c） 涉密会议的录音、转写与纪要生成不应交由人工智能处理。

6.3.4 待办拆解与派发

会议决议的待办拆解与派发应经使用者确认，并符合下列要求：

a） 应支持依据会议决议拆解待办事项并派发至责任人；

b） 派发结果应经使用者确认，不得由人工智能直接派发。

6.4 待办与日程管理

6.4.1 待办生成

待办与提醒的生成规则由使用单位设定，并符合下列要求：

a） 待办与提醒的生成应符合 3.4 的定义，提醒阈值与推送方式由使用单位按事项类别分别设定；

b） 应支持按事项、来源、时限等维度生成待办清单；

c） 待办清单应可导入导出，与办公自动化系统的事项保持一致；

6.4.2 时限提醒

时限提醒的节点与阈值由使用单位按事项类别设定，并符合下列要求：

a） 应支持依据办理时限设置提醒节点；

b） 提醒阈值应由使用单位按事项类别分别设定，本文件不作统一强制值；

c） 提醒应通过办公终端、即时通信等渠道推送，推送方式宜结合本地实际确定。

6.4.3 优先级排序

待办优先级排序规则应可配置、变更可留痕，并符合下列要求：

a） 应支持依据紧急程度、办理时限、事项重要性等维度对待办排序；

b） 排序规则应可由使用单位配置，规则变更应留痕。

6.5 知识沉淀与复用

6.5.1 经验总结

经验条目的形成、审核与入库应符合下列要求：

a） 应支持将已办结事项的办理过程、常见问题与处理方式整理为经验条目；
b） 经验条目应经使用者审核后纳入知识库，不应直接写入；
c） 经验条目应标注适用范围与适用条件。

6.5.2 知识检索与引用

知识库条目的引用应保持与来源一致，并符合下列要求：

a） 应支持在输出内容中引用知识库条目并标明来源；
b） 引用内容应保持与来源条目一致，不得改写后仍标注原来源。

6.6 事务跟办与提醒

6.6.1 任务跟踪

任务跟踪结果仅供使用者了解办理进展，并符合下列要求：

a） 应支持查询本人或授权范围内事项的办理进展与当前责任人；
b） 跟踪结果仅供使用者了解情况，不得作为督办依据；跨部门督办按《人工智能（AI）协同管理规范》执行。

6.6.2 台账填报辅助

台账草稿的生成与数据核对应符合下列要求：

a） 应支持依据使用者提供的数据生成台账草稿；
b） 台账数据的准确性由使用者核对确认，人工智能生成的数据不得直接报送；
c） 涉及统计口径的，应以使用单位规定的口径为准。

7 人机协同要求

7.1 辅助执行边界

人工智能办公秘书应用的辅助执行边界应符合下列要求：

a） 人工智能的处置动作应限定在 3.3 规定的辅助执行范围内，不应产生单独的对外效力；
b） 使用单位应明确授权清单，列明人工智能可执行、可建议、可提示三类动作；清单外的人工智能输出仅作为参考；
c） 授权清单应定期复核，岗位调整或制度修订后应及时更新；
d） 人工智能不应替代使用者作出具有行政效力的决定。

7.2 人工确认环节

人工确认环节的设置应符合下列要求：

a） 涉及发文、呈批、涉密处置、资金拨付、对外答复等环节的，应设置强制人工确认，不得提供跳过选项；
b） 人工智能输出内容在使用者确认前不得进入下一环节；
c） 人工确认的方式可以是逐项确认，也可以是对整篇文稿的审核确认，由使用单位按事项类别确定；
d） 确认与修改过程应留痕，记录确认人、确认时间与修改内容。

7.3 不得代为处置事项

下列事项不应由人工智能代为处置：

a） 涉及法定职责履行的事项，如以组织名义作出的行政决定；
b） 涉及涉密信息处理的事项；
c） 涉及对外正式行文的事项，包括以单位名义发出的公文、对外答复函件与正式函告；
d） 涉及个人权益处置的事项，如涉及考核、处分、薪酬的判定；

e） 涉及资金拨付、项目评审结论的事项。

7.4 过程可追溯

人工智能办公秘书应用的过程可追溯应符合下列要求：

a） 人工智能的每次处置动作应记录输入内容、调用模型、输出结果与人工干预情况；
b） 安全审计与记录管理应符合 GB/T 22239 的规定；涉及个人信息的处理记录应符合 GB/T 35273 的规定；
c） 记录保存期限不宜少于 1 年，具体期限由使用单位根据管理需要确定；
d） 应支持按使用者、时间、事项等维度进行责任追溯与统计分析。

7.5 禁止与限制事项

7.5.1 禁止代为决策

人工智能的决策与执行之间应保留人工判断，并符合下列要求：

a） 不应由人工智能作出决策后直接执行，决策与执行之间应保留人工判断环节；
b） 人工智能对事项的分类、排序、优先级判定结果，均应作为提示信息，不应直接触发处置动作。

7.5.2 禁止自动对外发送

任何对外发送行为均应经使用者确认，并符合下列要求：

a） 不应由人工智能在无人确认的情况下自动发送公文、对外函件、即时消息或电子邮件；
b） 对外发送的内容应经使用者确认，发送行为应记录发送人、发送时间与发送内容摘要。

7.5.3 禁止处理的数据类型

可输入人工智能服务的数据范围应从严限定，并符合下列要求：

a） 涉密数据不应输入人工智能服务处理；
b） 涉及国家秘密、工作秘密及不宜公开的敏感信息不应输入人工智能服务；
c） 涉及个人信息的数据处理应符合 GB/T 35273 的规定，法律法规另有规定的从其规定；
d） 未经使用单位批准，不得将本单位业务数据用于人工智能服务的模型训练。

7.5.4 禁止无人值守运行

辅助执行的运行方式应处于人工可控状态，并符合下列要求：

a） 人工智能辅助执行不应在无人值守状态下连续运行；
b） 需要持续运行的自动提醒类能力，其规则配置与阈值变更应经人工确认后生效；
c） 发现人工智能输出异常、重复输出或与事实明显不符的，应暂停相关能力并报技术支撑方核查。

8 安全管理要求

8.1 数据安全与保密

数据安全与保密要求应符合下列规定：

a） 应建立输入人工智能服务的数据分类规则，明确可输入、限输入与禁输入三类；
b） 应落实数据不出域要求，涉及本单位业务数据的处理宜在可控环境内完成；
c） 应对输入内容、输出结果与调用记录进行保密管理，保密管理要求应符合 GB/T 22239 的规定；
d） 密码应用应符合 GB/T 39786 的规定；
e） 涉密载体与涉密信息系统的处理按保密规定执行，不应通过人工智能办公秘书应用接入。

8.2 权限与审计

权限与审计要求应符合下列规定：

a） 应实施基于角色的访问控制与最小授权，知识库的检索范围应与使用者岗位职责相匹配；
b） 权限变更应履行审批并留痕；

c） 安全审计记录应覆盖登录、访问、操作、导出与权限变更；
d） 应支持异常与越权访问的监测告警，告警处置宜符合 GB/T 28827.1 的规定。

8.3 内容可信与标识

内容可信与标识要求应符合下列规定：
a） 人工智能生成的文字、数据、引用应标注为人工智能生成内容，使用者对外提供时应按规定标识生成合成属性；
b） 使用者应对人工智能输出中的事实、数据、政策条款进行核对，核对后方可对外使用；
c） 不应直接采信人工智能输出中未标注来源的内容；
d） 人工智能风险管理能力的评估宜符合 GB/T 46347 的规定。

8.4 生成式人工智能服务合规

生成式人工智能服务合规要求应符合下列规定：
a） 使用生成式人工智能能力的，宜选用已完成算法备案、且服务内容与本文件适用范围一致的服务提供者；
b） 生成式人工智能服务的通用安全要求宜符合 GB/T 45654 的规定；
c） 向公众提供的服务，应在服务界面及生成内容中按规定标识生成合成属性；内部办公场景的标识要求宜参照执行；
d） 应建立输入内容、模型版本、生成结果与人工处置过程的记录链，记录保存期限不宜少于 1 年；
e） 本文件不改变国家有关生成式人工智能服务管理的规定；具体要求按现行规定执行。

注：本条与《人工智能（AI）协同管理规范》相应条款保持一致，该文件同样以自述要求方式落地算法备案选用、生成内容标识与记录链保存义务。

9 运行与评价

9.1 部署与接入

部署与接入应符合下列要求：
a） 部署方式宜结合使用单位的保密要求与数据规模确定，涉密单位应按保密规定另行部署；
b） 与既有办公系统的接入应避免重复建设，宜复用本单位已有的公文与办公自动化系统；
c） 运行维护服务能力宜符合 GB/T 28827.1 的规定，明确服务范围、服务级别、交付物与验收判据。

9.2 培训与使用规范

培训与使用规范应符合下列要求：
a） 应对使用者开展人工智能办公秘书应用的使用培训，培训内容应包括能力边界、授权范围、禁止事项与人工确认要求；
b） 应通过宣贯材料、界面提示等方式明确告知禁止与限制事项；
c） 从业人员能力评价宜与岗位职责相匹配，能力评价通用要求可参见 GB/T 37696。

9.3 使用效能评价

使用效能评价应符合下列要求：
a） 宜从信息处理效率、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；
b） 评价指标的设定宜参照 GB/T 33850 的方法，具体指标与基线值由使用单位自行确定，本文件不作统一强制值；
c） 评价应区分“效率提升”与“责任转移”两种情形，不应以人工智能输出量替代对文档质量的评价。

9.4 持续改进

持续改进应符合下列要求：
a） 应建立使用反馈渠道，及时收集使用者在准确性、适用性、及时性方面的问题；

b） 改进措施应落实到知识库内容更新、规则阈值调整与授权清单修订；
c） 持续改进宜符合 GB/T 19001 关于 PDCA 循环与改进的要求。

附 录 A
（资料性）
人工智能办公秘书应用能力清单样表

人工智能办公秘书应用能力清单样表见表 A.1。

表 A.1 人工智能办公秘书应用能力清单样表

序号	能力域	能力项	典型输出	人工确认要求	建议授权方式
1	信息获取与整理	信息检索	文件清单与来源说明	检索范围确认	可执行
2	信息获取与整理	要点提取	办理要点与风险提示	抽取结果核对	可执行
3	信息获取与整理	材料归集	归集后的材料包	完整性确认	可执行
4	文档起草与辅助写作	提纲拟写	文档提纲	提纲确认	可建议
5	文档起草与辅助写作	段落起草	文稿初稿	全文审核	可建议
6	文档起草与辅助写作	文字润色	润色后文稿	实质性修改确认	可执行
7	文档起草与辅助写作	格式套用	套用模板的文稿	格式确认	可执行
8	会务辅助	议题征集	议题汇总	汇总核对	可执行
9	会务辅助	日程与通知	候选日程、通知草稿	发送前确认	可建议
10	会务辅助	记录与纪要	纪要草稿	定稿审核	可建议
11	会务辅助	待办拆解	待办派发清单	派发前确认	可建议
12	待办与日程管理	待办生成	待办清单	无须确认	可执行
13	待办与日程管理	时限提醒	提醒消息	无须确认	可执行
14	待办与日程管理	优先级排序	排序后的待办	无须确认	可执行
15	知识沉淀与复用	经验总结	经验条目	入库审核	可建议
16	知识沉淀与复用	知识引用	带来源的输出	无须确认	可执行
17	事务跟办与提醒	事务跟踪	进展查询结果	无须确认	可执行
18	事务跟办与提醒	台账填报	台账草稿	数据核对	可建议

注1：授权方式分“可执行”“可建议”两类。“可执行”指人工智能输出后不需人工操作即可生效；“可建议”指人工智能输出仅作提示，需人工采纳后方可生效。本表所列能力项为参考清单，使用单位可按岗位实际增删。

注2：本表所列能力项均不含 7.3 与 7.5 规定的不得代为处置事项与禁止事项。

附 录 B
（资料性）
典型提示词与人工复核要点示例

典型提示词与人工复核要点示例见表 B.1。

表 B.1 典型提示词与人工复核要点示例

能力项	提示词要素（示例）	人工复核要点	常见风险
要点提取	材料出处＋提取对象＋输出格式＋“不确定时标注存疑”	责任主体与时限是否与原文一致；存疑项是否已标注	将推测内容当作原文表述
提纲拟写	文种＋主题＋层级要求＋“仅拟结构不展开内容”	结构是否符合该文种的惯例；是否存在遗漏要件	生成的层级实为完整段落，影响后续审核
段落起草	已确认提纲＋要点清单＋语气要求＋“引用须标来源”	事实与数据是否均可追溯；政策条款引用是否准确	虚构数据；引用不存在的规定
文字润色	原文＋“仅作语句通顺与用词规范修改，不改变原意”	是否出现实质性改写；是否改变立场或口径	超出润色范围改写内容
纪要生成	录音转写稿＋“仅归纳已明确表述的内容，不作推断”	决议事项是否与发言原文一致；有无遗漏待办事项	将个人发言表述归纳为会议决议
台账填报	数据来源表＋口径说明＋“数据不确定时留空”	数据是否逐项核对；统计口径是否符合本单位规定	自行补全缺失数据

注1：提示词要素为本文件给出的参考模板，使用单位可结合实际调整。各要素中“不确定时标注存疑”“仅归纳已明确表述的内容”等限定语，是抑制人工智能编造内容的关键，不宜删减。

参 考 文 献

[1] GB/T 19000—2016 质量管理体系 基础和术语
[2] GB/T 25000.10—2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 10 部分：系统与软件质量模型
[3] GB/T 33136—2016 信息技术服务 数据中心服务能力成熟度模型
[4] GB/T 33477—2016 党政机关电子公文标识规范
[5] GB/T 33478—2016 党政机关电子公文应用接口规范
[6] GB/T 33480—2016 党政机关电子公文元数据规范
[7] GB/T 34960.5—2018 信息技术服务 治理 第 5 部分：数据治理规范
[8] GB/T 37696—2019 信息技术服务 从业人员能力评价要求
[9] GB/T 39362—2020 党政机关电子公文归档规范
[10] GB/T 43208.1—2023 信息技术服务 智能运维 第 1 部分：通用要求
[11] GB/T 45288.3—2025 人工智能 大模型 第 3 部分：服务能力成熟度评估
[12] T/CESA 1459 政务大模型系统功能要求（编号与名称以正式发布文本为准）
[13] 《党政机关公文处理工作条例》
[14] 《生成式人工智能服务管理暂行办法》（国家互联网信息办公室等七部门令第 15 号）
[15] 《广东省数字政府移动政务服务平台（“粤系列”）管理办法》
[16] 广东省政务服务和数据管理局《人工智能安全治理框架》2.0（全国网络安全标准化技术委员会技术文件）