横琴粤澳深度合作区行政事务局
公文辅助 AI 系统项目建设方案

第一章 项目概述

1.1. 项目名称

项目全称：横琴粤澳深度合作区行政事务局公文辅助 AI 系统项目。

项目简称（系统名称）：公文辅助 AI 系统。

1.2. 项目必要性分析

1.2.1. 提升数字政府行政效率与生产力的需要

合作区行政事务局共有综合事务处、文电处、人事管理处、公关礼宾处、研究协调处、合作区档案馆六个处室，普遍存在大量重复性文书工作（如公文撰写、数据整理等），传统人工处理效率低、易出错。一是自动化文档处理与生成，如综合事务处、文电处提出要以智能辅助写作应用加强公文初稿、摘要、简报等文档生成效率；二是细化专项写作工具能力，如文电处提出的智能公文排版助手和研究协调处提出的公文写作助手；三是加强写作素材专题库的内容，如财务法规知识库，深化合作区模板库的建立与应用，并动态更新知识库内容，定期抓取政府网站资料并分类集成。人工智能技术可实现自动化公文生成、智能校对、数据分类汇总，显著缩短公文文件处理周期，释放人力资源，满足高频次、高标准的内部办文需求。

1.2.2. 强化政府内部科学决策辅助的需要

当前政策制定缺乏实时数据支持。一是缺少跨部门数据的分类聚合与分析，如文电处的公函摘要分析助手；二是存在大量法规及政策文件的自动检索与匹配场景，需加强内部文件向内部知识的转化；三是需加强历史数据存储与快速检索，如研究协调处的公文素材知识库、督办事项助手的跟进情况，以更加便捷的手段快速联接重点专项任务摘要。人工智能大模型可整合历史数据与跨部门信息，提升精准性、效率，尤其在深合区一体化背景下，需动态响应大湾区政策联动需求。

1.2.3. 推动行政流程标准化与合规化的需要

各部门业务流程存在碎片化问题，如公文格式、督办事项，实现流程标准化，减少人为疏漏，确保行政行为的合法性与一致性。其次，提升内部办文合规性检测与标

准化输出，如遵循 2013 年第 7 号国务院公报《党政机关公文处理工作条例》和《党政机关电子公文格式规范》对公文的规范格式生成，各处室可以根据实际需求选择相应的模板，确保公文格式标准化。最后，加强深合区各管理局通用 AI 工具的适配与扩展，以确保其在不同应用场景中的高效运行，提高资源利用效率和安全保障水平。

1.2.4. 顺应数字化转型趋势，抢占区域发展先机

粤港澳大湾区已进入数字化转型加速期，各地政府竞相布局人工智能、大模型等新技术政务创新试点，实现行政审批全流程自动化；横琴深度合作区依托知识库建设，初步构建政策智能检索与公文协同平台。高新技术迭代速度加快，尤其在数字政府领域，智能应用正从单一工具应用向系统性、生态化方向演进，为加强深合区行政协同效能，整合跨区域政策联动与资源，公文辅助 AI 系统的建设既是响应国家战略的必然要求，更是突破区域同质化竞争、确立治理领先优势的核心路径。

1.3. 项目立项依据

1.3.1. 政策依据

1.3.1.1. 《数字中国建设整体布局规划》

2023 年 2 月中共中央、国务院印发《数字中国建设整体布局规划》，提出“到 2025 年，基本形成横向打通、纵向贯通、协调有力的一体化推进格局，数字中国建设取得重要进展。数字基础设施高效联通，数据资源规模和质量加快提升，数据要素价值有效释放，数字经济发展质量效益大幅增强，政务数字化智能化水平明显提升……”，特别强调数据要素价值有效释放和政务数字化智能化水平提升，行政大模型服务平台是面向党政机关以电子公文数据资源为核心的应用，完全符合数字中国整体布局规划倡导。

1.3.1.2. 《关于加快场景创以人工智能高水平应用促进经济高质量发展的指导意见》（国科发规〔2022〕199 号）

《指导意见》中发展目标明确，要场景驱动技术创新成效显著，通过场景创新促进人工智能关键技术和系统平台优化升级，形成技术供给和场景需求互动演进的持续创新力。形成政府、产业界、科技界协同合作的人工智能场景创新体系，场景创新主

体合作更加紧密、创新能力显著提升。

1.3.1.3. 《国务院办公厅关于全面加强新时代语言文字工作的意见》（国办发〔2020〕30号）

2021年11月30日，国务院办公厅发布《国务院办公厅关于全面加强新时代语言文字工作的意见》提出，大力推动语言文字与人工智能、大数据、云计算等信息技术的深度融合，加强人工智能环境下自然语言处理等关键问题研究和原创技术研发，加强语言技术成果转化及推广应用，支持数字经济发展。加强语言文字信息化平台建设，建设好全球中文学习平台，提供优质学习资源和信息服务资源。

1.3.1.4. 《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14号）

《国务院关于加强数字政府建设的指导意见》国发〔2022〕14号明确提出“加快推进数字机关建设，提升政务运行效能”“推进公开平台智能集约发展，提升政务公开水平”，行政大模型服务平台主要是通过将电子公文这项核心资源进行开发和利用，为各级领导、办公人员赋能，因此行政大模型服务平台将是数字政府建设很好的抓手。

1.3.1.5. 《广东省数字政府改革建设“十四五”规划》（粤府〔2021〕44号）

发展目标明确提出，基于整体政府视角，推动政府内部跨部门、跨层级的办文、办会、办事等提质增效，整体运行管理成本进一步降低……政府内部“一网协同”水平持续提升。以云计算、大数据、物联网、移动互联网为代表的新一代信息技术高速发展、交叉融合，应用创新空前活跃，5G、人工智能（AI）等新一代技术正持续向数字经济、数字社会渗透，必须顺应新技术发展趋势，充分发挥新一代信息技术在我省数字政府改革建设中的作用，以创新驱动经济社会高质量发展。

1.3.1.6. 《党政机关电子政务建设和管理“十四五”规划》

《党政机关电子政务建设和管理“十四五”规划》中指出要“建立健全电子文件形成、办理、归档利用、长期保存全生命周期管理机制，强化电子文件在数据资源中的基础地位，深化电子文件资源开发利用。建立电子文件管理与政务信息化工作协同发展机制，明确电子文件管理作为政务信息化项目立项申报要素，在政务信息化项目实施中同步落实电子文件管理要求。”

1.3.1.7. 《电子文件管理办法》

2023 年 6 月新颁布的《电子文件管理办法》中第十一条提到：【管理环节和原则】全过程管理且始终处于受控；第十五条中提到：【存储管理】分类分级，目录体系，授权访问机制，独立于业务系统进行保存；第十六条中提到：【利用】电子公文高效共享和有序开发利用。

1.3.1.8. 《党政机关公文处理工作条例》

2013 年第 7 号国务院公报《党政机关公文处理工作条例》中指出“【总则】适用范围为各级党政机关公文处理工作，包括公文的起草、审核、签发、管理、归档等流程；【公文种类】决议、决定、命令、公报、公告、通告、意见、通知、通报、报告、请示、批复、议案、函、纪要；【公文格式】要求包含份号、密级、紧急程度、发文字号、签发人、标题等 18 项要素，格式需符合国家标准（如 A4 纸张、规范用字等）；【行文规则】注重实效，不得越级行文（特殊情况需抄送被越机关）；【公文拟制】公文拟制包括公文的起草、审核、签发等程序；【公文管理】报告中不得夹带请示事项，涉密公文需严格保密措施，绝密级公文专人管理；复制、汇编需经批准，撤销或废止公文由发文机关决定。”

1.3.2. 标准规范

针对电子公文的规范化利用，国家出台了一系列标准，对电子公文的格式、元数据、标识、印章、归档等提出了明确要求和规范。

《电子文件存储与交换格式 版式文件》（GB／T 33190-2016 ）

《党政机关电子公文格式规范 第 1 部分 公文结构》（GB/T 33476.1-2016）

《党政机关电子公文格式规范 第 2 部分 显现》（GB/T 33476.2-2016）

《党政机关电子公文格式规范 第 3 部分 实施指南》（GB/T 33476.3-2016）

《党政机关电子公文标识规范》（GB/T 33477-2016）

《党政机关电子公文应用接口规范》（GB/T 33478-2016）

《党政机关电子公文交换接口规范》（GB/T 33479-2016）

《党政机关电子公文元数据规范》（GB/T 33480-2016）

《党政机关电子印章应用规范》（GB/T 33481-2016）

《党政机关电子公文系统建设规范》（GB/T 33482-2016）

《党政机关电子公文系统运行维护规范》（GB/T 33483-2016）

《党政机关电子公文归档规范》（GB/T 39362-2020）

《信息技术 OFD 档案应用指南》（ GB/T 42133-2022 ）

1.4. 项目目标

按照数字政府建设总体规划和本单位政务信息化规划，通过应用大模型的智能辅助能力，一是优化公文起草、撰写，大幅提高工作效率，提高公文质量与合规性。二是优化行政资源的配置和利用，减少重复劳动和资源浪费，提升整体办公效能。三是通过大模型的数据分析和智能推荐功能，提高决策的科学性和精准性。四是利用智能校对和修改功能，减少人为错误，提升公文的质量和合规性。深度利用高新技术手段推动政府数字化转型和智能化升级，打造现代化、智能化的政府办公体系。

1.5. 项目内容简介

本项目总体建设内容为基础设施服务、定制软件开发服务、系统业务运营服务和第三方服务，主要包括：

1.基础设施服务。主要内容为引入算力基础设施服务，支持 AI 能力赋能合作区电子公文交换系统，利用当地政务云服务能力。

2.软件开发服务。主要内容为公文辅助 AI 系统嵌入现有合作区电子公文交换系统的建设，公文辅助 AI 系统包括智能问答、智能搜索、公文审校、智能写作以及文件管理、配置管理、安全管理、系统管理、通用应用、智能插件；以及面向合作区不同单位、处室的权限管理、电子公文交换系统接口联调、单点登录、本地语料库建设和系统 UI 建设。

3.系统业务运营服务。主要内容为业务管理运营服务、数据处理运营服务。业务管理运营服务包括：业务场景运营、系统技术运营和管理支撑运营；数据处理运营服务包括数据治理服务、公共政务语料库、私有政务语料库、模型训练和其他资源库的更新与维护及驻场运维运营服务。

4.第三方服务。主要内容包括监理服务、第三方验收测评服务（含软件测评）、网络安全等级保护测评服务、商用密码应用安全性评估服务（含密码方案编制、方案评估、密码应用安全性评估）。

第二章 现状及需求分析

2.1. 现状及存在问题

2.1.1. 基础设施现状

本次规划部署到合作区政务云平台上，复用合作区已建设的计算、存储、网络以及安全等资源。

大横琴政务云平台是为合作区各单位对电子政务信息化提供计算、存储、网络、安全、数据库以及中间件等提供资源，政务云平台采用了云计算技术，具备设施、硬件、虚拟化计算资源。

目前，政务云平台已完成安全体系建设和网络安全等级保护建设，且已通过安全保护等级为第三级，业务信息安全为第三级，系统服务安全保护等级为第三级，整体网络安全防护能力较强。针对物理环境、通信网络、区域边界、计算环境等方面均已建成相应的安全防护措施。对于政务云上的服务器进出政务公共网的访问，都会经过政务云平台的安全边界的防护与监测，包括网络安全、租户安全、数据安全、密码安全等。

项目需采用高性能服务器集群，主要用于支持智能公文模型推理及政务应用系统的运行，GPU 服务器主要用于模型推理、微调和高性能计算任务，CPU 服务器用于日常政务应用系统的运行和数据处理，均采用符合信创要求的安全可靠的软硬件产品。

项目需采用高性能存储设备，用于公文数据的存储与管理，采用分布式存储系统，支持高并发访问和数据冗余，提供数据备份和恢复功能，确保数据安全。

2.1.2. 平台（系统）现状

本项目部署在合作区政务云平台上，充分利用合作区已建设的云资源。本项目计划建设公文辅助 AI 系统，并与执委会电子公文系统对接，进一步赋能各流程的智能化能力，执委会电子公文交换系统于 2024 年 4 月正式上线运行，为合作区执委会下九个局单位使用，部署在大横琴政务云平台上，执委会工作人员通过电子政务外网访问电子公文交换系统。

2.1.3. 运行维护管理现状

本项目为新建项目，不涉及运行维护管理现状。

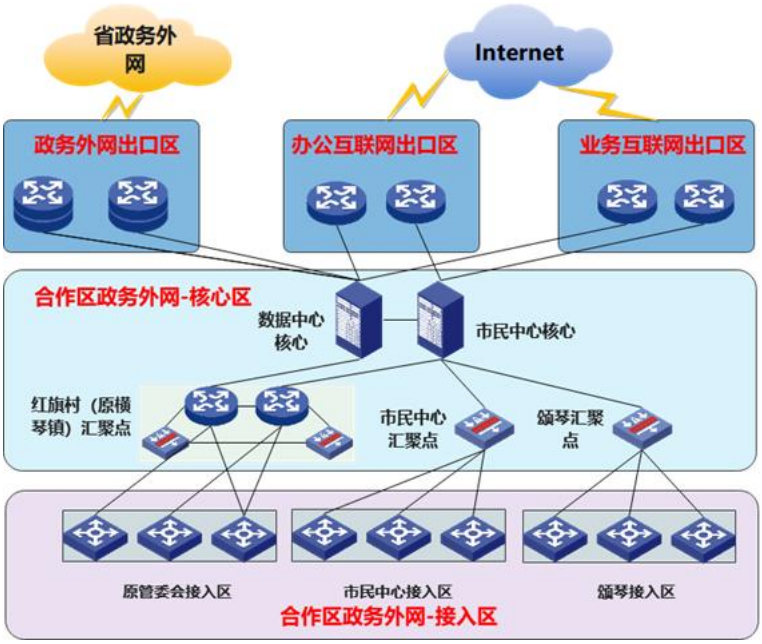
2.1.4. 系统业务运营服务现状

不涉及系统业务运营现状内容。

2.1.5. 密码应用和网络安全现状

密码作为保护网络与信息系统安全的重要手段，在身份鉴别、安全隔离、信息加密、完整性保护和抗抵赖性等方面发挥着不可替代的重要作用。

本项目计划使用商事服务局已建设的密码资源池提供密码服务，密码应用符合以下信息安全合规性和密码应用的要求，已按照密码应用安全性评估管理办法和相关标准，通过密码应用的安全性测评。网络安全复用政务外网的安全防护措施。



由出口区、核心区和接入区组成，初步形成政务外网“一网多平面”规范组网。

出口区：包含政务外网出口区用于提供合作区政务外网访问能力；办公互联网出口区提供合作区访问互联网能力；业务互联网出口区提供公众访问合作区业务系统能力。

核心区：以数据中心和合作区市民中心作为核心，汇聚层建设未完善，仅完成了

红旗村（原横琴镇）社区汇聚点的建设。

接入区：除合作区市民中心楼内的各单位接入外，分散在其他区域的接入点主要集中在红旗村（原横琴镇）原管委会区域、市民中心附近区域和颂琴区域。

2.1.6. 标准规范应用现状

不涉及。

2.1.7. 数据使用及共享现状

不涉及。

2.1.8. 存在问题

深合区电子公文交换系统沉淀了大量的公文文档、会议材料、政策法规等文件，每年增量公文并没有得到真正的分析和利用，无法为各级领导和办公人员提供赋能，主要存在以下问题：

2.1.8.1. 业务知识的可交互性有待提升

一是存在准确性的欠缺，由于公文文档、会议材料、政策法规等文件种类繁多，来源广泛，其内容的准确性难以得到完全保证。这导致在业务知识的传递和交互过程中，可能存在信息误导或理解偏差的情况，影响了决策的科学性和效率。二是对知识积累的理解有限，常规电子公文交换系统整理的知识积累主要停留在表面层次，缺乏对深层次知识和业务逻辑的挖掘，这导致在业务知识的交互过程中，难以形成全面、深入的理解，限制了知识的有效应用和价值发挥。三是对经验的依赖程度较高，往往依赖于个别专家或资深人员的经验，这种经验驱动的方式缺乏统一的标准和流程，使得业务知识的传递和共享受到限制。过度依赖经验还可能导致知识的片面性和主观性，为了提高业务知识的可交互性，需要建立更加科学、系统的知识管理和共享机制，减少对经验的过度依赖，提升知识的标准化和客观性。

2.1.8.2. 内部文档检索效果较差

相关知识推荐不够详尽，用户在检索内部文档时，往往期望能够获得与查询关键词高度相关且详尽的知识推荐，当前的系统在这方面表现欠佳。检索模块可能不够智

能，无法准确捕捉到用户查询的真实意图，推荐结果与用户需求存在偏差。缺乏摘要能力，在内部文档检索过程中，本地电子公文系统缺乏对文档的摘要能力，需要花费更多时间成本来理解每篇文档的内容，以确定其是否与自己的查询需求相匹配，严重降低工作效率，大概率导致使用者错过关键词或重要文档。

2.1.8.3. 公文审校流程繁琐

在处理重复性任务或复杂内容时，往往会反复的修改和迭代，特别是在非标准化的公文内容中容易出现遗漏。传统的校对方法或人工校对可能难以充分理解内容的上下文，尤其是在涉及多语言内容时，这可能会导致审核的不准确性。此外，在面对特定行业术语或专业表达时，可能缺乏足够的背景知识库支持，从而无法准确判断其使用是否恰当。这可能导致一些专业性强、语境特殊的表述被误判，增加了后续人工复核的工作量。同时，在处理学术型文本时，也可能因为缺乏对这些表达方式的深刻理解，而做出过于机械或片面的判断，影响了文本的整体质量和传达效果。

2.1.8.4. 文件分散未深度利用

海量电子流转文件沉淀于电子公文系统中，但这些数据大多处于静态存储状态，缺乏深度分析和挖掘，系统未能充分利用，未将公文数据转化为有价值的决策支持信息，难以实现单个主题的脉络梳理和整体呈现。未建立专题公文知识库，在查找和利用特定主题相关的公文时，需要耗费大量的时间和精力手动检索和筛选，使得信息的获取变得困难且效率低下，不仅影响了工作的效率，也限制了公文数据在组织内部的流通和价值发挥。

2.1.8.5. 存量公文数据格式多样

由于历史原因，当前电子文件的格式以多种格式存在，如 doc/docx/wps/pdf/ofd/jpg/jpge/ceb/cebx/sep/txt 等格式，这些格式的文件在打开、阅读、签批、安全控制、深度利用等方面都存在极大的困难。PDF、OFD、图片格式（如 jpg、jpeg）文件难以直接进行文本提取和语义分析，而 doc、docx 等格式文件虽然便于编辑，但在与其他系统集成时又面临格式转换的难题，格式多样性不仅限制了数据的高效流通和共享，在阅读体验上排版和显示效果差异，一定程度上降低了工作效

率。

2.1.8.6. 技术和业务融合不通

当前系统的技术架构与功能设计尚未与业务场景紧密融合，难以适应各部门及岗位的特定需求。系统无法实时更新最新的政策法规和业务知识，这使得公文处理的合规性和准确性难以得到保障。在跨部门协同办公时，公文流转效率低下，重复劳动和信息滞后的问题依旧存在。此外，由于技术与业务之间的脱节，导致系统在处理复杂业务逻辑时割裂。例如，公文审校流程中标准排版、套红等环节，往往需要人工干预、叠加处理才能完成，增加了人力成本，也延长了公文处理的周期。

2.2. 需求分析

2.2.1. 业务需求分析

大模型智能化已成为推动政府部门办公模式改革的重要手段。为了提高行政办公效率、优化资源配置、增强决策的科学性和精准性，我局计划建设行政事务局公文辅助 AI 系统底座和能力平台。通过大模型的应用，执委会工作人员可以更加高效地完成公文的起草、撰写、校对和修改工作。这将大大提升政府工作效率，减少人为错误和延误，确保公文的质量和合规性。同时，这也将有助于提升政府的透明度和公信力，进一步推动政府数字化转型和智能化升级。

本期项目主要面向执委会的行政事务局工作人员开放使用，可授权的用户数暂为 400 人，未来将面向执委会所有工作人员(约 2000 人)，按照 20（QPS）并发设计公文辅助 AI 系统底座建设。

2.2.2. 基础设施需求分析

系统资源需求表

序号	服务名称	服务配置	数量(台)	计算方法和依据	备注
1	GPU 裸金属服务器	国产算力服务器	1	见下文	
2	数据库服务器	CPU：32C 内存：64G 存储：500GSSD	2	见下文	
3	Web 应用服务器	CPU：32C 内存：64G 存储：500GSSD	3	见下文	
4	模型应用服务器	CPU：64C 内存：128G 硬盘：1TSSD	1	见下文	
5	数据管理服务器	CPU：32C 内存：64G 存储：500GSSD	1	见下文	
6	数据治理服务器	CPU：32C 内存：64G 存储：500GSSD	1	见下文	
7	对象存储	5T	1	见下文	
8	安全	主机安全、VPN、堡垒机、数据库安全审计等支持等保三级要求	1	见下文	
9	密评	国密服务器等，支撑国密认证测试的配套设备	1	见下文	
10	操作系统	银河麒麟 V10	8	见下文	
11	数据库软件	达梦数据库 V8	2	见下文	

电子公文系统部署在电子政务外网，本期计划授权的用户数约为 400 人，最大并

发数约为 20 人(峰值)，假定单用户 2K Token/次，基于 AI 推理算力需求≈2×模型参数量×数据规模×峰值倍数，估算需要 4.6PFlops 算力，建议配置 1 台 16 卡华为昇腾 910B GPU 服务器。详细测算如下：

1. 模型算力需求估算

经验系数

通常，在大语言模型推理阶段，每 10 亿参数大约需要 3 - 6 TFLOPS（每秒万亿次浮点运算）的算力。这里我们取中间值，按每 10 亿参数 4.5 TFLOPS 来计算。

模型 1：办公写作、搜索、校对的 32B 大模型

320 亿参数的模型算力需求约为： 13*4.5=144TFLOPS

模型 2：政策流程知识库问答 72B 模型

720 亿参数的模型算力需求约为：72*4.5=324TFLOPS

2. 考虑并发情况

假设 20 个并发用户对两个模型的使用是均匀分布的，即每个模型有 10 个并发用户同时进行操作。

模型 1 办公 32B 模型并发算力需求

10*144=1440 TFLOPS

模型 2 政策流程知识库问答 72B 模型并发算力需求

10*324=3240 TFLOPS

所以总并发算力需求：

两个模型并发算力需求相加可得：3240+1440=4680 TFLOPS

3. 华为 910B 算力设备参数

华为 Ascend 910B 芯片单卡算力在 FP16 精度下为 320 TFLOPS。

4. 计算所需设备数量

所需华为 910B 设备数量 = 总并发算力需求 ÷ 单卡算力，即

4680/320=14.625 卡

由于设备数量必须为整数，并且为保证系统能稳定应对并发请求，需要向上取整，所以大约需要 16 卡华为 910B 算力设备。

综上所述，拟按照 1 台 16 卡华为 910B，或选择相等算力的 GPU 服务器。

本项目业务应用考虑采用合作区政务云云服务器作为基础设施，包括以下云资源。

1 台 GPU 裸金属服务器提供算力支持；

2 台数据库服务器用于承载主备数据库业务；

3 台 Web 应用服务器用于提供 AI 应用服务（1 台提供入库、查询，1 台提供编辑校对，1 台提供政策流程问答应用和知识库）；

1 台模型应用服务器，部署模型，协同 GPU 服务器支持 AI 应用。

1 台数据管理服务器，用于承载数据；

1 台数据治理服务器，用于提供数据治理服务；

配置对象存储和配套网络、安全等服务。

数据存储量：

基于以上电子公文数据量分析，针对本项目建设内容以及数据量初步分析，本期用户注册数约为400人，每人每周处理10个电子公文文件，平均每个公文文件为5MB，未来行政大模型服务平台每年产生的公文数据量大约为 1TB，考虑到模型对数据结构化处理需要额外 1TB 空间，本地数据处理需要 2TB 空间，以及部署数据管理和配套工具需要额外 1TB 空间，建议存储按照 5TB 申请云资源。存储数据可为 SSD ，备份数据可为对象存储。考虑数据备份需要额外 5TB 空间。

综上所述拟存储 5TB SSD 和 5TB 对象存储。

2.2.3. 公共支撑能力需求分析

充分复用横琴合作区已建统一身份认证能力、电子公文交换系统组件能力。

1、统一身份认证系统（AD）复用需求

复用合作区统一身份认证系统，实现用户身份的统一管理和单点登录（SSO）。用户身份同步，从统一身份认证系统同步用户信息（如姓名、部门、角色）。单点登录集成，提供标准接口实现用户通过统一身份认证系统一键登录新建系统。权限分级管理，基于统一身份认证系统的角色权限体系，实现公文辅助 AI 系统的分级权限控制（如用户、管理员）。

2、电子公文交换系统组件能力复用需求

复用电子公文交换系统的组件能力，实现公文的高效流转与交换。公文推送接口，将新建系统生成的公文草稿自动推送至电子公文交换系统进行审批。审批状态同步，实时获取电子公文交换系统中的审批状态（如已提交、已审批、已驳回）。历史公文调用，从电子公文交换系统调用历史公文数据，用于智能推荐和参考。

2.2.4. 功能性需求分析

2.2.4.1. 人工智能模型底座应用需求

大模型应用底座旨在构建高性能、可扩展的能力支持层，为上层应用提供强大的计算能力和算法支持。需实现公文语义理解、政策术语识别、智能写作等功能，为智能公文工具提供底层能力支撑。此外，底座还需支持动态扩展和弹性调度，能够根据业务需求灵活调整资源分配，确保系统在高并发场景下的稳定运行。

2.2.4.2. 智能化服务应用需求

为提高公文数据使用效率，系统需提供多种智能化服务，具体需求包括智能问答、公文智能检索、公文智能比对、公文敏感词检测、公文智能纠错、公文辅助写作、公文一键排版等智能化服务。智能化服务还需提供适用于电子公文交换系统协同的接口集成能力，可将公文辅助写作、公文智能校对、公文智能摘要、公文一键排版、公文智能检索等智能化能力以页面嵌入的形式在电子公文交换系统中开放服务，或为将来其余接入的第三方应用进行赋能。

2.2.4.2.1. 智能问答

智能问答应用需准确理解用户意图，识别关键词和上下文关系，以多轮交互式问答，根据上下文信息补充提问或澄清模糊问题，在返回答案的同时，推荐其总结来源，帮助用户获取更全面的信息。

2.2.4.2.2. 智能搜索

智能搜索需支持根据关键字快速检索公文辅助 AI 系统公开的相关历史文件，方便机关工作人员对电子公文的即时需求，从专题数据库中快速检索出最相关的答案，支持全文检索和语义检索。

2.2.4.2.3. 公文审校

公文审校需对政策术语、法规依据、敏感内容进行校验，检查公文中编写的内容是否准确、有效，并提供校对原因类别。还需根据《党政机关电子公文格式规范》支持对文种格式、标点符号检查等进行审校，在公文中高亮显示错误或问题内容，并提供具体修改建议。

2.2.4.2.4. 智能写作

公文辅助写作需符合简单公文、复杂公文的写作逻辑，包括模版、素材、润色、续写等功能，提供符合国标标准的电子公文格式，提供各种套红模板入口。公文一键排版需对于发文拟文人员拟稿正文的字体、分级标题、标点符号、段落样式等按标准要求排版后送领导审批。

2.2.4.3. 系统对接需求

系统对接服务需实现公文辅助 AI 系统与执委会电子公文交换系统的对接，通过标准化接口，实现用户身份同步、公文数据交换等功能。需支持在公文辅助 AI 系统中起草公文后，直接推送至电子公文交换系统进行审批流转。系统需支持与政策法规库、公文模版库等数据源的对接，确保公文内容的准确性和权威性。同时，系统对接服务还需考虑安全性与稳定性，确保数据传输过程中的加密处理，防止信息泄露。在接口设计上，需遵循高效、易用原则，减少对接复杂度，提升用户体验。此外，系统对接服务应具备良好的扩展性，以应对未来可能新增的数据源或功能需求，确保系统的长期稳定运行。

2.2.4.3.1. 文件权限管理需求

对于入库的文件，需要可以控制用户对特定数据或文档集的访问权限，有效保护敏感信息，防止数据泄露。同时考虑用户权限与用户角色分类授予，颗粒度按照文档及文件夹实施，并支持对文件权限管理申请、审批、设置等。

2.2.4.3.2. 接口联调需求

本系统必须支持与执委会电子公文交换系统接口对接和联调，实现电子公文交换系统相关 API 对接，包括权限、流程、数据、安全体系、用户体系等。与上述系统对接应支持灵活的对接方式，保持接口稳定和兼容，减少对已有系统的干扰。

2.2.4.3.3. 单点登录设计需求

本系统应支持单点登录设置，新系统应与省统一身份认证系统对接，或支持现有深合区统一身份认证系统，对于相关系统的用户，能在电子公文交换系统和本系统间，实现登录一次即可访问另一系统，无需多次认证。同时，用户登录应有日志记录，实现登录行为的查询和审计。

2.2.4.3.4. 系统 UI 联动配置需求

本项目开发的系统需与协作的另一系统在用户界面（UI）上保持高度一致，从整体视觉风格到交互细节，为用户提供统一、连贯的使用体验。实现视觉风格统一、交互方向一致，界面整体规划，色彩图形留白间距统一规划，确保界面设计美观、简洁，符合人体工程学和美学原则，提升用户满意度。

2.2.4.4. 文档管理需求

本项目应支持通过文库和目录查看和管理系统内的文档，设置用户对文档的操作权限，包括权限设置、移动、查看详情、在线阅读、移除、下载、编辑功能。

2.2.4.5. 配置管理需求

2.2.4.5.1. 文档入库配置需求

本项目的相关文件在入库前，须配置入库方案，应支持对文件入库位置、处理方式、审核机制等内容进行设置；支持对入库文件进行标准化处理，实现对入库文件向量化解读；支持自定义入库方案配置，用于不同类型文档入库后的数据处理。节点配置项包括格式转换、文字识别、文件拆分、信息提取、人工处理，审批等。

2.2.4.5.2. 基础数据配置需求

本项目应支持对文档类型、元数据和标签等数据配置管理，用于支持不同维度的文档入库与展示。同时系统应支持配置文档类型、格式、元数据字段。

2.2.4.6. 数据处理需求

2.2.4.6.1. 基础元数据处理需求

数据处理服务需通过自动化工具和人工辅助相结合的方式，对合作区的历史公文、政策文件、案例库等数据进行结构化处理，构建高质量的语料库。数据处理服务还需

支持对公文关键字段（如标题、发文单位、政策依据）进行标注，为智能搜索和语义理解提供数据基础。

由系统管理员提前设置元数据项，电子公文的元数据分为核心元数据以及扩展元数据。核心元数据包括公文标识、文种、份号等 18 种，扩展元数据包括人名、机构名称、职务名称等操作。基础元数据管理具体需求为元数据建立、元数据维护、元数据值的管理、文件类型的配置与管理。

元数据建立需支持对元数据的创建，包括对元数据的名称、定义、赋值类型、值域、编码体系等。元数据维护需要对元数据进行导入导出、修改更新等操作。元数据值的管理需提供多种默认值，方便元数据的输入、支持对元数据值的验证机制，可实现对元数据的迁移与管理。文件类型的配置与管理需要对文件保管要求、利用控制、文件种类或者重要元数据属性上存在较多共性而设置的灵活的管理层次。

2.2.4.6.2. 数据标准化处理需求

为保证各个电子公文资源规范管理和利用，需要建立项目范围内，统一的文件格式封装、元数据、文件编码、文件目录和系统接口，按照国家版式文档格式要求党政机关单位须对电子公文进行 OFD 格式标准化处理，实现各用户单位可按业务需要快速共享公文资源，包括公文 OFD 标准格式转换、公文元数据字段提取、公文正文内容碎片化加工。

非标准化公文须按照要求进行标准化格式转换，需提供对常见格式包括文本格式、PDF 格式、图片格式等公文的转换服务。可支持多格式转换、套版转换、批量转换、多引擎转换、高速转换等功能。公文元数据字段提取需实现对电子公文 18 项核心元数据的抽取，包括：公文标识、文种、份号、密级和保密期限、紧急程度、发文机关标志、发文字号、签发人、标题、主送机关、附件说明、发文机关或签发人署名、成文日期、附注、抄送机关、印发机关、印发日期、发布层次等。公文正文内容碎片化加工需要按照段落、句子对公文正文进行碎片化加工，方便后续搜索定位、智能推荐等场景使用。

2.2.4.6.3. 多维度分类需求

公文辅助 AI 系统提供多维度分类，帮助用户通过条件筛选快速、准确地找到所需要的知识。通过类型、主题、时间、发文部门、紧急程度等维度，定位公文范围，帮助用户快速定位所搜索的相关内容。多维度分类具体需求包括类型分类、主题分类、时间分类、职能部门分类、紧急程度分类等。

2.2.4.7. 安全管理控制

系统将部署在电子政务外网，与互联网隔离，安全管控需求具体包括传输安全，内容安全，存储安全，文档防泄漏，模型训练必须本地化严禁数据离开政务云。传输安全需对传输过程中的身份信息进行安全管控。内容安全需要对接入、收到的电子公文进行安全管控。存储安全需对公文库资源的存储及备份进行安全管控，保证数据安全。

2.3. 非功能性需求分析

2.3.1. 平台响应速度需求

响应时间指标包括页面响应时间和数据响应时间。

根据业务处理类型的主要划分为三类：交互类业务、查询类业务和大数据量批处理类业务。

（1）交互类业务

交互类业务有较高的响应要求，根据业务复杂性分为日常交互和审核校对类业务，具体响应时间参考如下：

日常交互类业务：不大于 3 秒；

审核校对类业务：不大于 5 秒；

（2）查询类业务

查询类业务由于受到查询的复杂程度、查询的数据量大小等因素的影响，需要根据具体情况而定，具体响应时间参考如下：

简单查询：不大于 3 秒；

复杂查询：不大于 5 秒；

（3）大数据量批处理类业务

大数据量批处理类业务由于数据查询量大、并发性要求高等因素的影响，系统性能要求较高，具体响应时间参考如下：

10000 字以内业务批量处理：首 token 输出时延不大于 5 秒；

10000 字以上复杂批量业务处理：首 token 输出时延不大于 10 秒。

2.3.2. 平台可扩展性需求

系统设计和实施要充分考虑网络、硬件的扩展需要、应用系统二次开发的需要以及支持未来可能出现的组织调整的需要。系统应采用开放的可扩充模块结构，保证以后可以方便地升级和不断增加新功能、增加容量、以及在同一平台上扩充其他业务应用功能。

垂直扩展能力：应用系统可通过升级服务器硬件、网络、存储等提升承载能力。

横向扩展能力:应用系统架构上可通过在集群中增加服务器提高相应的承载能力)，业务应用支持通过增加应用实例实现横向扩展。支持弹性伸缩功能，支持快速扩容。

2.3.3. 平台易用性需求

根据本项目工作的需要，在技术的使用和产品的选择方面要考虑其技术的成熟性，同时在产品方面要考虑适用和实用，保证技术、性能满足项目建设需要。

1．应用各模块间对同一内容的表达保持一致、相同操作保持一致，并尽可能与其他系统保持一致。

2．概念、内容、提示信息清晰、准确，容易理解。功能名称、图标、按钮应该直接、明了，没有歧义。

3．用户可以直接根据界面提示使用，无需过多的参考使用说明书和参加培训。

4．系统的人机界面友好、界面设计科学合理以及操作简单等，操作按扭、快捷键、图标等遵循一致的规范、标准，按钮的位置、颜色等符合其重要程度。

5．提供的功能和内容方便用户发现、查找和获取，无隐藏得很深不容易被发现的功能或链接。必要时提供功能地图、清单页面。

6．页面输入顺序、查询和显示格式、重要业务数据的相关性排列顺序符合用户

习惯及常见标准。

2.3.4. 平台可靠性需求

在日常工作中，需要通过 7×24 小时不间断的系统性维护服务，确保本期项目具有良好的安全性和可靠性，同时结合备份恢复、入侵监测、防火墙等工作，共同构建起多层次，全方位的安全保障体系，系统可靠率为 99%。另外，同时通过日常维护使系统具备一定的容错性，避免由于误操作或其他原因导致的系统错误。允许进行多用户操作，且其性能指数隔离，即一个用户的操作不能因为其性能降低影响到另一个用户，不能形成死锁行为。

2.3.5. 平台高可用需求

为保证业务系统的连续性，行政大模型应支持容错、自恢复、高可扩展能力，允许应用系统从不可避免的硬件、软件错误中恢复，确保应用系统的正常运行和数据存储的高可靠。平台系统设计应当遵循 SOA 的设计，以松耦合和服务化构建整体架构设计以达到开放性的目的，秉承可重复的业务任务或服务整合的思想。系统整体设计在保持业务连续性方面应具备以下条件：系统软件采用模块化结构，模块之间的通信应按规定接口进行。任何一层的任何一个模块的维护和更新以及新模块的追加都不应影响其他模块。组件采用松耦合架构，对部分组件进行功能扩展，不影响整体架构。

2.4. 安全需求分析

2.4.1 安全可靠需求

基础设施作为行政大模型服务平台中计算资源、存储资源、网络资源和安全设备的提供者，是整个行政大模型服务平台中的基础组成部分，主要包括计算设备、存储设备、网络设备、操作系统等四大类。行政大模型服务平台内基础设施建设的基本原则是提高硬件资源的利用率，降低系统总体能耗，以低成本的方式提供对海量计算的支撑，并从基础层面保证系统的高可用性。

当前，国产化硬件存在多种不同的技术路线，基于不同的技术路线，各硬件厂商也发布了不同的国产化硬件设备，随着全国产化服务器的日渐成熟，国产化服务器芯片包括但不限于飞腾、鲲鹏、龙芯等已经达到生产应用标准。国产化操作系统包括中

标麒麟、银河麒麟、统信 UOS 等，也实现了对多种国产化硬件的全面支持。

在安全可靠替代项目实践中可以发现，单一技术路线可能会带来一定的技术和管理风险。根据行政大模型服务平台安全可靠替代的整体要求，行政大模型服务平台需要适配多种不同技术路线的国产化计算设备和操作系统。

2.4.2 平台安全性需求

综合提升电子公文资源安全保障能力，实现电子公文分类分级管理，精细化设置访问权限，强化访问控制，确保电子公文存储、共享利用、传输交换的安全。

国家《网络安全法》于 2017 年 6 月 1 日正式施行，并于 2019 年 12 月 1 日已正式执行了“网络安全等级保护制度 2.0”。所有网络运营者和关键信息基础设施运营者均有义务按照网络安全等级保护制度的要求对系统进行安全保护。等保 2.0 充分体现了“一个中心、三重防御”的思想。因此，需从一个“安全管理中心”，三重防御“安全计算环境、安全区域边界、安全网络通信”多角度出发，结合可信计算安全技术实现全方位的系统安全防护能力。完成建设后的行政大模型服务平台需符合等级保护三级建设标准。

平台将部署在电子政务外网，保障数据传输安全可控；整体安全管控分为用户权限管控和数据安全管控。用户安全管控包括：用户排序管理，角色安全保密管理，系统公文权限管理。数据安全管控包含：日志审计跟踪管理，数据传输安全管理，内容安全管理，存储安全管理，文档防泄漏管理等。

2.4.2.1 信息安全等级保护要求

国家《网络安全法》于 2017 年 6 月 1 日正式施行，并于 2019 年 12 月 1 日已正式执行了“网络安全等级保护制度 2.0”。所有网络运营者和关键信息基础设施运营者均有义务按照网络安全等级保护制度的要求对系统进行安全保护。等保 2.0 充分体现了“一个中心三重防御”的思想。因此，云数据中心安全建设应从一个“安全管理中心”，三重防御 “安全计算环境、安全区域边界、安全网络通信”多角度出发，结合可信计算安全技术实现全方位的系统安全防护能力。电子政务外网按照《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》定为等保三级。

针对信息安全等级保护的要求，系统建设应从物理安全、网络安全、边界防护、计算环境、国密、机构管理、人员管理、运维管理满足需求。

本项目建设过程中，需按照等级保护 2.0 三级标准要求进行等保建设和测评。

等保建设包括：网络安全建设、安全区域边界设计、安全计算环境设计和安全管理中心设计。

等保测评包括：

1、完成信息系统安全等级保护定级备案工作，编制信息系统安全等级保护定级报告及备案资料，并取得国家信息安全等级保护主管部门出具的信息系统等级保护备案证；

2、完成信息系统安全等级保护差距测评服务，根据测评结果出具差距测评报告；

3、根据安全整改结果，完成验收测评并提交符合国家信息安全等级保护主管部门要求的验收测评报告，通过国家信息安全等级保护主管部门的最终测评验收；

4、按照实际情况提供渗透测试服务，提交渗透测试报告。

2.4.2.2 密码应用需求分析

政务云按照《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》定为等保三级，根据国家密码法要求：国密应用安全性评估（简称“密评”）应当与网络安全等级测评制度相衔接。因此电子政务外网不仅需要满足《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》三级系统相关要求，还需要满足《信息系统密码测评要求》中三级系统相关要求。电子政务外网将参照《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中三级系统要求，进行密码应用需求分析。

- 安全风险分析

应用和数据面临的风险包括：密码服务平台被非法人员登录，导致平台被入侵；传输或存储的业务数据被其他应用获取、被外部攻击者非法获取；访问控制信息、应用日志记录被非法篡改，以掩盖非法操作。

通常在政务外网访问业务系统，使用用户名+口令方式，没有安全身份校验机制以及没有对传输通道进行加密的问题，依靠操作系统和信息系统自身的安全设计，无法解决身份伪造、连接欺骗等可能存在的应用篡改、数据非授权访问、数据篡改，甚

至数据泄漏等问题，只有对访问终端、客户端（如浏览器），链路都添加符合国密要求的密码加密和身份验证模块，才能够确保系统应用和数据的安全。

互联网区的业务系统，互联网区 PC 端用户通过非国密浏览器使用用户名+口令方式进行登录身份鉴别，均未使用密码技术对登录用户进行身份鉴别，存在应用被非授权人员登录风险。

● 密码应用需求

1、身份鉴别

服务端部署符合国密相关国家、行业标准要求的身份认证系统，通过身份认证系统，实现对 PC 端登录应用用户的安全身份鉴别，防止非授权人员登录。

2、数据传输安全

本次项目系统为在政务外网内使用，不存在互联网传输需求，无法提供有效的基于域名认证的 https 证书，因此在数据传输方面，依托政务外网本身非授权不可访问的安全性实现对业务调用的安全访问以及数据安全传输。

3、数据存储机密性

系统内的关键数据包含用户鉴别数据、用户基础数据、非结构化电子公文数据等，需要在政务外网区、互联网区分别实现系统关键数据的存储机密性保护。

4、数据存储完整性

系统中的关键数据包含用户鉴别数据、重要配置数据、日志记录等，需要在政务外网区、互联网区分别实现系统关键数据的存储完整性保护。

2.4.2.3 数据安全需求分析

在数据安全方面，服务平台应按照等级保护的基本要求，对服务平台涉及的数据安全进行脆弱性识别及安全防护。其具体的内容如下：

- 数据完整性：操作系统、数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的完整性保护情况。
- 数据保密性：操作系统和数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的保密性保护情况。

2.5. 标准编制需求分析

不涉及标准编制。

第三章 总体设计

3.1. 系统架构设计

3.1.1. 总体架构设计

公文辅助 AI 系统的总体架构一共分为七层，分别为基础设施层、数据支持层、公共支撑层、模型支持层、业务应用层、应用入口层和用户层，如下图所示：

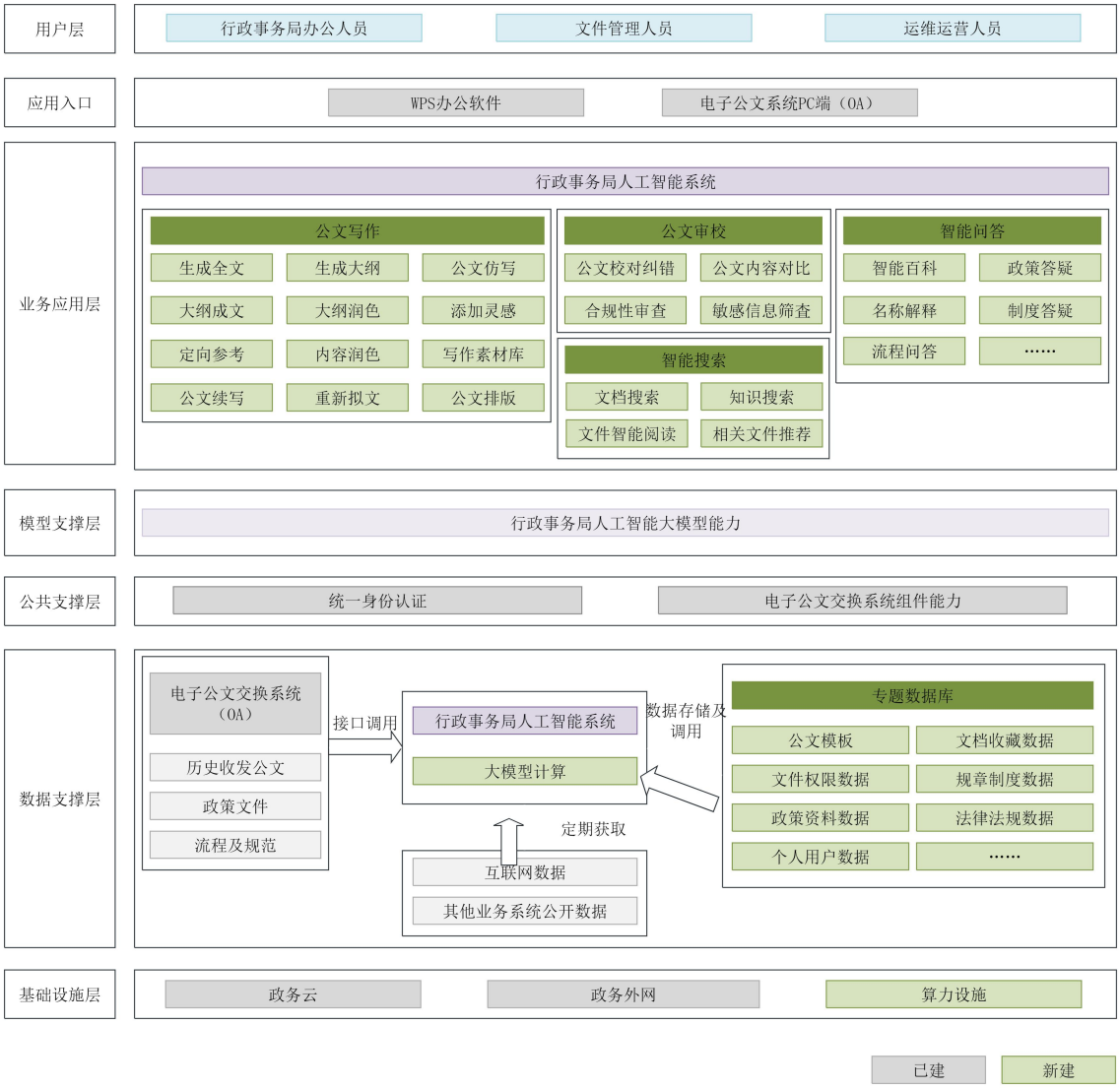


图 总体架构设计图

用户层：面向行政事务局办公人员、文件管理人员及运维运营人员，提供多终端

统一入口，包括 WPS 办公软件、电子公文系统 PC 端（OA）及公文辅助 AI 系统。通过角色权限分级管理，满足不同用户群体的核心需求，如公文起草、审核、查询、运维等，确保系统与用户实际工作场景无缝衔接。

应用入口：用户可从 WPS 客户端、电子公文系统（OA）PC 端入口进入使用公文辅助 AI 系统的相关功能，页面集成到电子公文系统中，实现用户的单点登录无感使用。

业务应用层：聚焦公文全生命周期管理与智能辅助决策，建设公文写作、公文审校、智能问答和智能搜索核心功能模块。同时集成写作素材库、文档搜索、知识搜索等工具，支持从灵感启发到成文落地的全流程智能化升级。

模型支撑层：依托行政事务局人工智能大模型，通过融合政策文件、历史公文、规章制度等多源数据，持续优化模型在公文生成、语义理解、知识推理等场景的精准度与适应性，为上层业务应用提供可靠的 AI 能力底座。

公共支撑层：本期项目遵循集约化原则，复用电子公文系统（OA）已建设的执委会用户体系实现统一身份认证和账号的单点登录。整合电子公文交换系统接口调用等基础组件能力，实现跨系统数据互通与服务协同。建设专题数据库，包括公文模板、文档收藏数据、历史收发公文等，提供标准化数据调用接口，保障业务流与数据流的高效联动，降低系统间集成复杂度。

数据支撑层：构建多维度数据资源池，充分利用原有电子公文系统相关文件资料，建设涵盖政策文件库、法律法规库、文件权限数据、互联网公开数据等结构化与非结构化数据库。通过定期更新与动态治理机制，确保数据时效性与权威性，为知识检索、公文写作等场景提供高质量数据供给。

基础设施层：基于政务云与政务外网环境，部署弹性可扩展的算力设施，满足大模型推理的高性能需求。通过网络安全防护与数据加密技术，保障系统运行稳定性及敏感数据合规性，为上层应用提供安全可靠的基础环境支撑。

3.1.2. 应用架构设计

应用架构设计分为四层分别是：应用场景及功能、模型支撑层、技术运营支撑层、数据层，如下图所示：

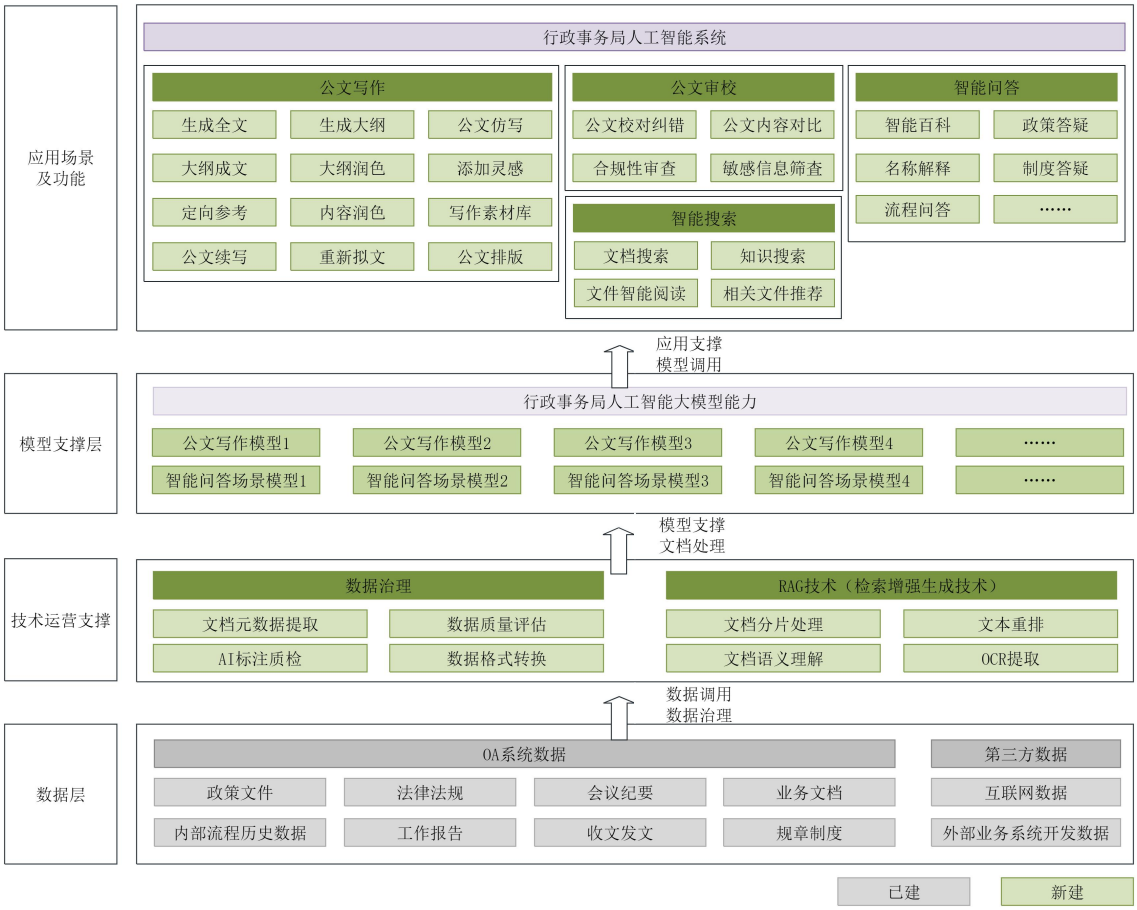


图 应用架构设计图

应用场景及功能：本次规划建设的行政事务局公文辅助 AI 系统功能包含公文写作、公文审校、智能搜索和智能问答四个模块。其中公文写作可以实现 AI 的智能化写作辅助功能，包含大纲和全文的编写，以及根据用户的要求完成公文草拟和排版等任务。公文审校可以实现通过 AI 的大模型算法辅助用户进行公文的审阅和校核，且可以提供公文比对的功能。智能搜索可根据用户输入的检索要求已有文档和知识的搜索，并提供文档推荐、智能阅读等功能。智能问答可根据用户的提问在知识库里进行检索，实现政策答疑、制度答疑和名词解释等功能，用户在咨询政策和内部流程相关内容时可根据已有的政策文件及梳理的内部流程办法等数据整理答案进行解答并推荐相关内容给用户查阅。

模型支撑层：通过构建大模型能力，实现本期建设功能的智能化学习和深度学习，通过相关数据梳理、模型优化、应用优化等运营工作实现模型输出结果的精准化和智

能化，实现相关场景的智能决策。完成成熟的公文写作和智能问答类的大模型可以更好的支撑应用功能的实现。

技术运营支撑：为支撑四大业务场景应用的技术能力，分为两部分的技术能力，第一部分为数据治理能力，具备对公文、制式文档的元数据提取、格式转换、数据治理评估等能力。第二部分为 RAG 技术，具备文档分片处理、文本重排、文档语义理解、OCR 提取等能力。

数据层：负责对接各种的用户业务数据，包括 OA 系统已有数据的调用，如：公文档案、规则制度、会议材料、业务文档等数据接入，同时支持互联网数据的收集和单项输入，通过数据治理后为大模型推理提供优质精准的数据来源。

3.1.3. 数据架构设计

数据架构设计共分为 6 层，分别是应用场景层、数据开放层、数据治理层、数据预处理层、数据存储层、源数据采集层，如下图所示：

图 数据架构设计图

应用场景层：本次规划建设的公文辅助 AI 系统功能包含公文写作、公文审校、智能搜索和智能问答四个模块。其中公文写作可以实现 AI 的智能化写作辅助功能，包含大纲和全文的编写，以及根据用户的要求完成公文草拟和排版等任务。公文审校可以实现通过 AI 的大模型算法辅助用户进行公文的审阅和校核，且可以提供公文比对的功能。智能搜索可根据用户输入的检索要求已有文档和知识的搜索，并提供文档推荐、智能阅读等功能。智能问答可根据用户的提问在知识库里进行检索，实现政策答疑、制度答疑和名词解释等功能，用户在咨询政策和内部流程相关内容时可根据已有的政策文件及梳理的内部流程办法等数据整理答案进行解答并推荐相关内容给用户查阅。

数据开放层：负责将治理好的数据通过 API 网关、共享数据库加工好的数据集开放给上层应用场景使用。

数据治理层：使用大模型治理数据平台收集各类工作文档并进行数据血缘分析、数据质量管理、数据模型设计、元数据提取等数据治理工作。

数据预处理：使用 OCR、实体抽取等工具提取 PDF、Word 等类型的文档内容，并对文档内容进行知识采集预处理。

统一数据存储：负责存储大模型平台收到的各类文档、数据。

数据源采集：负责支持各类数据传输协议对接，负责接入源数据，包括结构化数据和非结构化数据。

3.1.4. 业务架构设计

图 业务架构设计图

业务架构设计分为五层，分别是用户层、应用入口、业务场景层、业务支撑层、业务存储层，具体如下：

1.用户层：包括事务局人员、文件管理人员和运营运维人员。

2.应用入口：包括 WPS 用户端和电子公文交换系统用户端

3.业务场景层：

公文写作：实现公文的起草、编辑、校对、签发、流转等全生命周期管理。包括素材引用、大纲生成、文件生成、公文仿写、公文润色等，起草格式必须遵循《党政机关电子公文格式规范》

智能搜索：整合各类办公数据，利用先进的搜索算法和语义理解技术，为用户提供精准、高效的信息搜索服务。用户可通过关键词、语义等方式搜索公文、制度文件、会议纪要等资料，搜索结果按照相关性和重要性进行排序展示。

智能问答：基于政策流程知识库和大模型的推理能力，为用户提供政务办公相关问题的解答。无论是政策解读、业务流程咨询，还是日常办公疑问，用户都能通过该功能获得准确、详细的回答。

公文审校：提供公文校对纠错、公文内容对比、合规性审查和敏感信息筛查能力，助力用户提高公文的准确性、合规性和合理性。

4.业务支撑层：

用户管理：负责用户信息的录入、更新、删除等操作，管理用户账号、权限、角色等。根据用户所在部门、职位等因素，为用户分配相应的操作权限，确保系统安全、有序运行。

权限管理：对系统内各类功能和数据进行细粒度的权限控制。通过设置不同的权限组，如管理员权限、普通用户权限、只读权限等，保障敏感信息不被非法访问和操作。

模型管理：对办公模型和问答模型进行日常运维管理，包括模型配置、性能优化等。确保模型的稳定性和准确性，及时根据业务需求对模型进行调整和优化。

5.业务存储层：

公文切片分类存储：将已完成流程的公文按照规定的格式和分类方式进行存档，便于后续查询和审计。支持对存档公文进行全文检索，方便用户快速定位所需文件。

数据存储：定期备份以及所有存储数据不能向云外流出。

知识库：对业务过程中产生的知识、经验、解决方案等进行整理和沉淀，丰富知识图谱内容。通过知识沉淀，实现知识的复用和传承，提高整体业务水平。

3.1.5. 网络架构设计

用户从政务外网进入，经核心交换机过汇聚交换机，再经过楼层、机柜交换机后进入到对应的虚拟机中获取到相关组件服务。

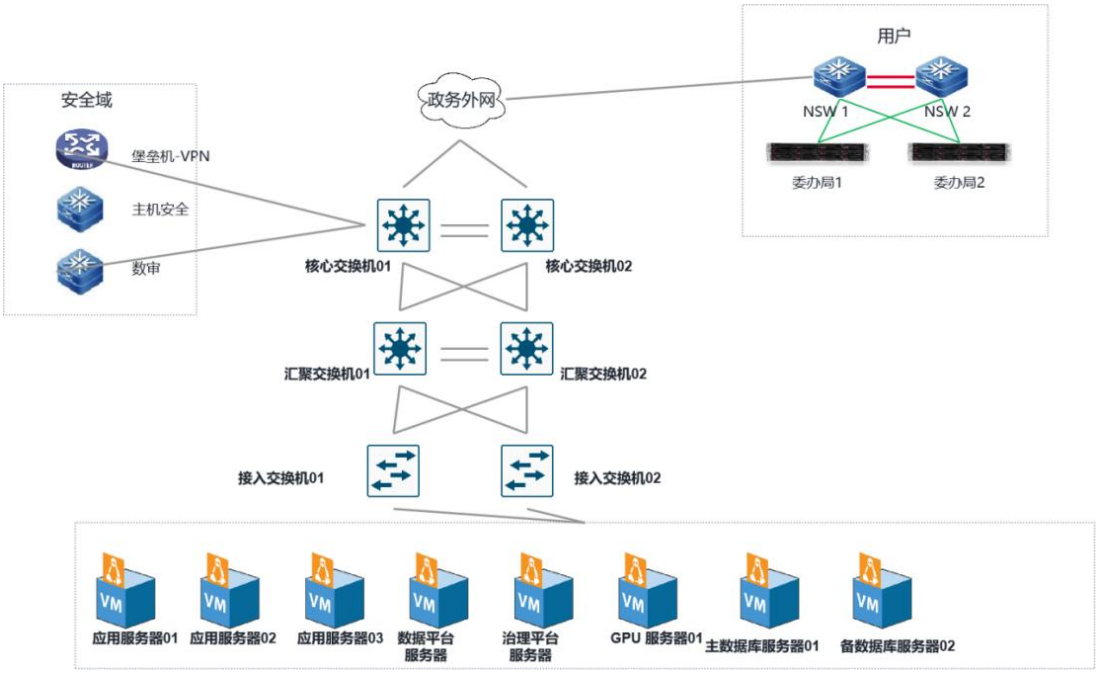


图 网络架构设计图

3 台应用服务器：使用 3 台 web 应用服务器，分别服务于部署业务前端应用（包括 1 台政策流程问答服务器、1 台公文信息搜索查询服务器、1 台公文写作和审校服务器）部署问答应用、web 服务、写作服务、校对服务、查询服务等关系型数据库、图数据库、minio、校对服务等其他辅助 IT 应用。

1 台数据平台服务器：该服务器用来部署用于数据接入数据开放的服务器。包括数据管理和工具，如 OCR 服务等。

1 台数据治理服务器：该平台用来部署数据治理平台，对接入公文数据进行治理，完成治理后将治理的数据形成结构化数据存入数据库中。

2 台数据库服务器：部署模型所需关系型数据库。如达梦和 PG 数据库，2 台数据库互为主备。

1 台 GPU 应用服务器：使用 1 台 GPU 用来部署 LLM 模型，包括办公模型和通用问答模型，支撑上层应用使用 AI 服务。

1 台智算服务器：部署 GPU 算力卡，为模型和工具提供算力支持服务。

其他还需要配套的安全、网络相关设备。支持网络安全等保三级、国密安全和必要存储空间等。安全需要至少具备堡垒机、VPN、数据库安全审计、主机安全、网络

防火墙等功能；国密需要具备国密安全服务器密码机等设备。

用户通过 SSL VPN 访问政务外网上的公文辅助 AI 系统上的智能问答、智能搜索、公文审校、公文写作等应用。也可通过本地 WPS 客户端调起公文辅助 AI 系统的相关应用。

3.1.6. 安全架构设计

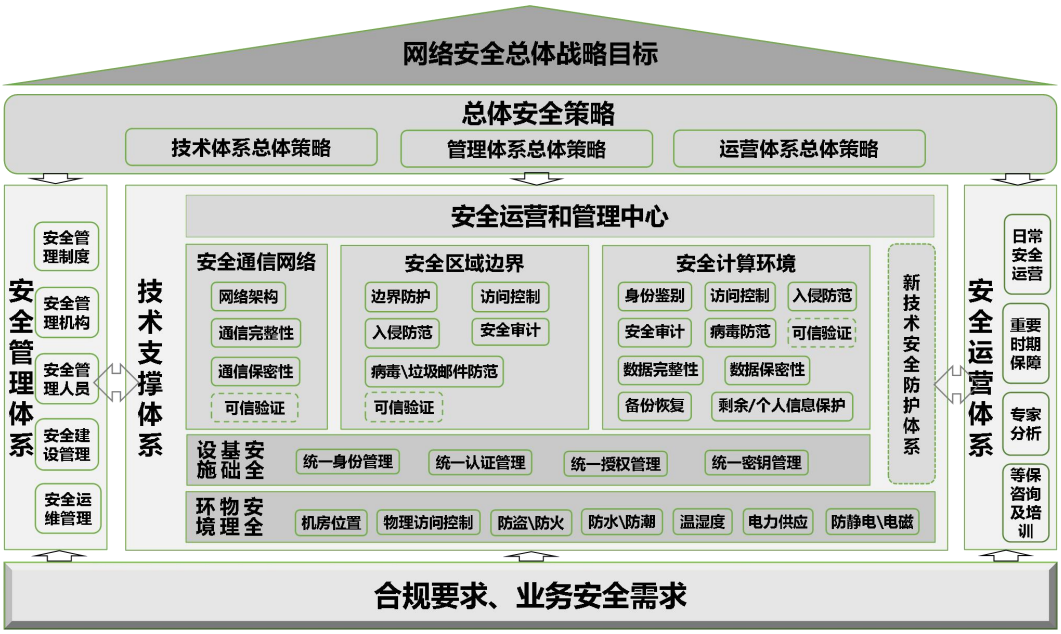


图 安全架构设计图

本系统安全保障体系是以“一个中心、三重防护、三个体系”为核心指导思想，构建集防护、检测、响应、恢复于一体的全面的安全保障体系。其中；

“一个中心”是指安全运营管理中心，即构建先进高效的安全运营管理中心，实现针对系统、产品、设备、策略、信息安全事件、操作流程等的统一管理。

“三重防护”是指构建安全区域边界、安全计算环境、安全通信网络三维一体的技术防御体系。

“三个体系”是指形成安全技术体系、安全管理体系、安全运营体系，三个体系相互融合、相互补充，形成一个整体的安全防御体系。其中，安全管理体系是策略方针和指导思想，安全技术体系是纵深防御体系的具体实现，安全运营体系是支撑和保障。

安全体系建设考虑复用云安全体系。本项目建设系统安全管理方面融入政务云安全管理体系，遵守政务云安全管理制度。技术上使用政务云配置安全防护技术和软硬件能力，包括堡垒机、VPN、防火墙、数审等安全设备能力。项目后续运营工作，严格按照运营体系要求开展运营工作，做好安全防护工作。项目建设完成前，配合做好等保三级和密评测试的工作。

3.1.7. 系统性能设计

1、支持同时在线 400 用户，正常 20 个并发用户的性能要求；

2、响应指标，用户登录系统响应时间在 3 秒内，一般 Web 页面调用的响应时间 3 秒以内；

3、服务器内存平均占用率小于 50%，最大并发时小于 75%;

4、系统支持 7×24 小时运行。

3.1.8. 数据备份方案

本项目备份系统复用政务云平台的备份系统进行普通文件和数据库文件的备份存储，存储技术采用政务云平台所提供的存储技术，包括块存储和对象存储，存储网络则依托政务云平台基础网络。

计算方法及依据：

针对本期项目审验数据，按照存量数据 500G，每月数据新增约 10G 计算，全年 120G 新增业务，则每年所需的存储空间约为 620G，加上本应用部署所需空间，约为 1TB 存储需求，再结合数据标注和知识库应用需要增加 4TB 存储空间，每年所需存储空间约为 5TB。

本项目建议采用每周增量备份、每月全量备份，备份数据保存 6 个月。

本期项目生产运行环境需要共 5TB 的存储空间，同时按照备份原则，需要云上备份空间 5TB，以满足存储完整备份的需要。因此共需要 10TB 存储空间。

3.2. 系统整合与业务协同

本次建设的公文辅助 AI 系统，与执委会电子公文系统实现技术对接，计划部署在云资源池中，采用现有的基础网络资源、网络安全防护设施、运维管理体系等，同

时为相关应用提供统一的存储资源及灾备能力。

本次项目的建设所需服务器资源、密码资源池服务向商事服务局申请，在本项目中不再产生政务云资源租赁费用和密码资源池服务费用。

结合 GB/T22239-2019《信息安全技术网络安全等级保护基本要求》、GB/T25070-2019《信息安全技术网络安全等级保护安全设计技术要求》云计算扩展要求。

本项目公文辅助 AI 系统与电子公文交换系统的整合与协同，旨在实现公文起草、校对、排版等全流程的智能化与自动化，提升政府工作效率和公文处理质量。

（1）起草阶段

智能辅助写作：用户在公文辅助 AI 系统中使用智能写作功能（如素材推荐、格式校验）完成公文起草。系统自动检查公文内容的政策合规性和格式规范性，提高审核效率。

（2）校对阶段

智能审校自动检测公文中的政策、格式、逻辑等问题，并提供修改建议，从而提升公文质量和审核效率。支持不同版本公文的比对，高亮显示新增、删除、修改部分，保障校对原因、校对操作智能化。

（3）排版阶段

默认支持基于党政机关公文格式标准(GB/T9704—2012)对文本内容一键排版，也可对目标排版样式进行设定，实现一键自动调整文本格式和排版风格，排版助手可对落款、附件等进行微调，排版完成后可对多种公文类型进行套红，套红后可上传至电子公文交换系统进行流转。

3.3. 技术路线及部署设计

公文辅助 AI 系统采用 JAVA、C++等语言开发，全面支持信创基础软硬件环境和国产 GPU，综合运用了大语言模型、大数据、自然语言处理等关键技术，内置 ES 服务、Redis 服务、Nacos 服务以及 OCR、Convert 等服务，为用户提供智能、高效、安全的“问、搜、审、写”智能办公服务。

3.3.1. 自然语言处理（NLP）

运用自然语言理解（NLU）技术，解析用户输入的意图与需求，精准识别出关键信息。利用自然语言生成（NLG）技术，将处理后的信息转化为结构化的公文内容，确保公文的准确性和规范性。NLP 技术还能有效支持公文中复杂语义的理解与分析，提升系统对公文内容的深度把握能力。借助语义分析技术，深入挖掘文本的含义，确保所生成的公文内容与语境和逻辑保持一致。NLP 技术还能实现公文的语义分析，通过不断优化，系统能够持续学习并提升对公文语境的理解能力，确保公文内容的准确性和专业性。

3.3.2. 大语言模型

大语言模型（Large Language Model，简称 LLM），指使用大量文本数据训练的深度学习模型，可以生成自然语言文本或理解语言文本的含义。大语言模型可以处理多种自然语言任务，如文本分类、问答、对话等，是通向人工智能的重要途径。目前大语言模型采用与小模型类似的 Transformer 架构和预训练目标（如 Language Modeling），与小模型的区别是增加模型大小、训练数据和计算资源。

LLM 主要应用：

1.自然语言理解：通过语法词汇、句法语义、语境等相互作用，使计算机能够理解人类语言。

2.文本生成：LLM 技术在文本生成方面的应用可以在文本摘要、翻译和自动化写作等方面进行适用。

3.3.3. 检索增强生成技术（RAG）

公文辅助 AI 系统通过 RAG（Retrieval-Augmented Generation）技术提供系统内文档数据的检索功能，即通过向量搜索机制，根据输入的文本块从候选的文档数据中找到并返回概念相似的文本。

检索增强生成技术是一种使用真实世界信息改进 LLM 输出的技术，是大多数基于 LLM 的工具的重要组成部分，能够直接利用检索得到的文档信息进行内容生成，无需进行额外的训练，但其准确性存在一定问题。

公文辅助 AI 系统引入了 GraphRAG（图基检索增强生成）技术来保障检索结果的准确性。

GraphRAG 是一种结合了知识图谱和大型语言模型（LLM）的检索增强生成（RAG）技术，旨在通过将结构化和非结构化数据相结合来增强生成式 AI 的表现。GraphRAG 通过构建知识图谱，从非结构化文本中提取结构化数据，使得模型能够更好地理解和处理复杂信息，能够更精确地检索和生成与上下文相关的响应，特别适合处理需要深度上下文理解和复杂关系分析的任务。

GraphRAG 适用于需要复杂信息检索和生成的应用场景，如问答系统、对话系统等。通过结合检索系统和生成模型，GraphRAG 能够在生成过程中从外部数据库或文档中检索相关信息，结合上下文生成更精确的输出。

相较于仅向量 RAG，GraphRAG 的优势主要分为三大类：

1.准确度更高且答案更完整（运行时间/生产优势），可以进一步消除模型幻觉

2.一旦创建好知识图谱，那么构建和维护 RAG 应用都会更容易（开发时间优势）

3.可解释性、可追溯性和访问控制方面都更好（治理优势）。

3.3.4. ES 服务

ES 服务是指 Elasticsearch 服务，它是一个开源的分布式搜索引擎，主要用于提供数据存储和快速检索功能。Elasticsearch 使用分布式架构来存储数据，通过分片和复制技术提高性能和容量，适用于处理大规模数据和高并发请求。

主要功能和应用场景：

数据存储和检索：Elasticsearch 可以存储大量结构化和非结构化数据，并提供快速的搜索和检索功能。它使用 Apache Lucene 作为核心，支持复杂的查询和聚合操作。

实时性能：Elasticsearch 具有出色的实时性能，可以在毫秒级别快速响应查询请求，适用于需要快速反馈的场景。

数据分析和聚合：它提供强大的数据分析和聚合功能，支持各种统计和聚合操作，帮助用户从海量数据中发现有价值的信息和模式。

扩展性和可靠性：Elasticsearch 具有高度的可扩展性和可靠性，可以水平扩展到数百甚至数千个节点，支持主从复制和故障转移机制，确保数据的高可用性和可靠性。

公文辅助 AI 系统使用 ES 技术实现多维检索和数据分析。

3.3.5. Redis 技术

Redis 是高性能内存数据库，以内存存储、多种数据结构和单线程模型等技术原理为基础，适用于缓存、会话存储、消息队列等应用场景。

Redis 的核心技术：

内存存储：Redis 将数据存储在内存中，因此具有极高的读写性能。同时，Redis 支持持久化存储，可以将内存中的数据定期或实时地保存到磁盘上，保证数据的持久性。

丰富的数据结构：Redis 支持多种数据结构，包括字符串、哈希表、列表、集合、有序集合等。这些数据结构不仅简单高效，而且功能强大，可以满足各种不同的应用场景需求。

单线程模型：Redis 采用单线程模型来处理客户端请求，通过事件驱动机制实现高并发的处理能力。这种设计保证了 Redis 的简单性和性能，并且能够有效地利用多核处理器的优势。

事件驱动：Redis 使用事件驱动模型处理客户端请求和网络通信，通过非阻塞 I/O 和事件循环机制实现高效的网络通信和请求处理。

公文辅助 AI 系统使用 Redis 技术实现缓存和快速数据访问，可以缓存一些经常被访问的数据，如用户的常用公文模板、系统的配置参数等。通过将这些数据存储在 Redis 中，可以大大提高系统的响应速度，减少对后端存储系统的压力。

3.3.6. 微服务架构

微服务技术为整个系统提供基础服务支持。公文辅助 AI 系统中的基础服务涵盖了多个方面，包括 ocr 应用、web-reader 服务、convert 服务、用户管理、权限管理等。对文档处理识别、查看预览、合成处理等方面提供服务支持，在用户管理方面，负责用户账号的创建、删除、修改密码等操作。权限管理则确保不同级别的用户只能访问和操作他们被授权的功能和文档。文档管理涉及到对用户创建和存储的公文文档进行分类、存储、检索等操作，确保文档的安全性和可访问性。

（1）微服务的主要特点

1）单一职责

每个微服务都需要满足单一职责原则，微服务本身是内聚的，因此微服务通常比较小。系统应用中每个微服务按业务逻辑划分，每个微服务仅负责自己归属于自己业务领域的功能。

微服务的开发通常与 DevOps 结合在一起，比如根据亚马逊给出的经验，一个微服务应该可以由一个 Two Pizza Team 负责设计、开发、测试和运维。

2）自治

一个微服务就是一个独立的实体，它可以独立部署、升级，服务与服务之间通过 REST 等形式的标准接口进行通信，并且一个微服务实例可以被替换成另一种实现，而对其它的微服务不产生影响。

（2）微服务的优势

1）逻辑清晰

这个特点是由微服务的单一职责的要求所带来的。一个仅负责一项很明确业务的微服务，在逻辑上肯定比一个复杂的系统更容易让人理解。

逻辑清晰带来的是微服务的可维护性，在对一个微服务进行修改时，能够更容易分析到这个修改到底会产生什么影响，从而通过完备的测试保证修改质量。

2）简化部署

在一个单块系统中，只要修改了一行代码，就需要对整个系统进行重新的构建、测试，然后将整个系统进行部署。而微服务则可以对一个微服务进行部署。

这样带来的一个好处是，可以更频繁的去更改软件，通过较低的集成成本，快速的发布新的功能。

（3）可扩展

应对系统业务增长的方法通常采用横向（Scale out）或纵向（Scale up）的方向进行扩展。分布式系统中通常要采用 Scale out 的方式进行扩展。因为不同的功能会面对不同的负荷变化，因此采用微服务的系统相对单块系统具备更好的可扩展性。

（4）灵活组合

在微服务架构中，可以通过组合已有的微服务以达到功能重用的目的。

（5）技术异构

在一个大型系统中，不同的功能具有不同的特点，并且不同的团队可能具备不同的技术能力。因为微服务间松耦合，不同的微服务可以选择不同的技术栈进行开发。

同时，在应用新技术时，可以仅针对一个微服务进行快速改造，而不会影响系统中的其它微服务，有利于系统的演进。

（6）高可靠

微服务间独立部署，一个微服务的异常不会导致其它微服务同时异常。通过隔离、融断等技术可以避免极大的提升微服务的可靠性。

3.3.7. 机器学习与深度学习

使用大量公文样本数据训练机器学习模型,特别是深度学习模型(如 Transformer、BERT 等），以学习公文的语言风格和结构。通过深度学习模型，系统能够识别并模仿不同种类的公文风格，从而生成符合特定要求的公文。同时，这些模型还能自动检测并纠正公文中的语法、拼写等错误，提高公文的质量。机器学习与深度学习技术的结合，使得系统在处理复杂、多变的公文任务时表现出更高的灵活性和准确性。此外，随着训练数据的不断增加和模型的持续优化，系统的公文处理能力将进一步提升，为用户提供更加智能、高效的公文处理体验。生成模型，采用生成式预训练模型（LLM 系列），生成符合规范的公文内容。这些生成模型在接收到特定的指令或上下文信息后，能够自动产生连贯、专业的公文文本。LLM 系列模型不仅擅长捕捉语言的统计规律，还能够理解公文中的深层语义关系，从而生成既符合语法规则又具备专业内涵的公文内容。此外，通过微调这些预训练模型，可以使其更好地适应不同行业、不同部门的公文写作需求，进一步提升公文的针对性和实用性。

3.3.8. 模型可测性

1、智能问答：Top3 答案召回率≥90%，用户修正频次<2 次/千字；智能写作：格式合规率 100%，文本重复率≤20%；知识库检索：多模态特征匹配率≥95%。

2、自动化测试框架：模拟 200 并发压力测试。

3.3.9. Java 技术体系及 B/S/D 三层模型

在技术体系上选用 Java 体系结构，采用 B/S/D 三层模型进行应用系统的开发。Browser/WebServer/Database 是解决信息服务以及交互相应动态服务最适用的一种应用模型，实现了真正意义上的瘦客户，大大简化了应用系统的分发、配置管理和版本管理工作。

Java 平台企业版（JavaPlatform，EnterpriseEdition）J2EE 是一套全然不同于传统应用开发的技术架构，包含许多组件，主要可简化且规范应用系统的开发与部署，进而提高可移植性、安全与再用价值。

J2EE 核心是一组技术规范与指南，其中所包含的各类组件、服务架构及技术层次，均有共通的标准及规格，让各种依循 J2EE 架构的不同平台之间，存在良好的兼容性，解决过去企业后端使用的信息产品彼此之间无法兼容，企业内部或外部难以互通的窘境。

J2EE 的优越性为：

（1）基于 JAVA 技术，平台无关性表现突出

（2）开放的标准，许多大型公司已经实现了对该规范支持的应用服务器。如 BEA，IBM，ORACLE 等。

（3）提供相当专业的通用软件服务。

（4）提供了一个优秀的专业级应用程序框架，对快速高质量开发打下基础。

3.3.10. 国产化适配

公文辅助 AI 系统运行在纯国产环境中，涉及到 CPU、操作系统、数据库等方面的集成适配。本项目将针对国产环境做基础适配测试，包括麒麟操作系统、统信操作系统，海光、鲲鹏、兆芯、飞腾、龙芯等 CPU，达梦、人大金仓数据库，并根据国产软硬件环境的现实能力对系统中使用的相关技术，进行算法调优，保障在国产环境下稳定高效运行。

针对国产 GPU 显卡，从操作系统内核、GPU 驱动、GPU 功能支持、模型适配和算法优化等多个维度进行性能提升，以保障在有限资源的情况下，支持高并发需求。

第四章 建设内容

4.1. 基础设施内容

4.1.1. 公共基础设施

本项目计划配置云服务器 8 台，包括 web 应用服务器 3 台、模型应用服务器 1 台、数据库服务器 2 台、数据平台服务器 1 台、数据治理服务器 1 台。

配置存储 10TB 用于存储电子公文库的公文、系统应用、知识库数据、业务数据、用户数据、系统配置数据及工具等内容。详见下表。

序号	设备及软件	主要配置	数量	单位	说明
一	基础设施				
（一）	公共基础设施				
1	数据库 服务器	CPU：32C 内存：64G 存储：500GSSD	2	台	行政大模型服务平台基础功能(入库、查询)
2	Web 应用 服务器	CPU：32C 内存：64G 存储：500GSSD	3	台	行政大模型服务平台拓展功能(编辑、校对)
3	模型应用 服务器	CPU：64C 内存：128G 硬盘：1TSSD	1	台	数据库安装及存储
4	数据管理服务器	CPU：32C 内存：64G 存储：500GSSD	1	台	部署数据平台工具
5	数据治理服务器	CPU：32C 内存：64G 存储：500GSSD	1	台	部署数据治理服务
6	存储	按照实际文件量 1:5 配置，按照 1TB 已有公文数据，配置 5TBssd，考虑备份，额外配置 5TBSSD 或对象存储	1	套	建议 10TB 高性能 SSD 含备份

4.1.2. 专业基础设施服务

本项目按并发算力需求分析计划配置 1 台算力服务器。

序号	设备及软件	主要配置	数量	单位	说明
（二）	专业基础设施				
1	智能 AI 服务		1	台	智能问答、智能搜索、智能协作、智能审校等功能须 GPU 算力，按照 20 用户并发配置

4.2. 软件开发内容

4.2.1. 定制软件开发服务

4.2.1.1. 用户范围

本期项目用户覆盖行政事务局所有科室的办文用户，预计用户数量为400人。主要业务科室为文电处，其余科室均有收文和办文工作人员。

4.2.1.2. 公文辅助AI系统

4.2.1.2.1. 智能问答

4.2.1.2.1.1. 智能百科

基于已上传的政策文件库、法律法规库及历史公文数据，构建垂直领域的行政知识库，支持对行政专业术语、业务流程、职能规范等内容的即时检索与深度解析。通过自然语言交互，可快速获取标准化解释、关联文件及典型案例，为办公人员提供一站式知识查询服务，降低信息获取门槛。

4.2.1.2.1.2. 政策答疑

对接实时更新的政策法规数据库，支持对国家级、地方级及行业级政策的精准解读。用户可通过自然语言提问，系统自动提取政策核心条款，匹配适用场景并提供执行要点、申报流程等指导信息，确保政策理解与执行的规范性与一致性。

4.2.1.2.1.3. 制度答疑

深度整合机构内部规章制度、流程规范及历史审批数据，构建动态问答引擎。针对内部管理制度，包括电子公文交换系统中已有的内部审批、财务报账等业务，提供智能答疑与操作指引，并结合实际案例说明规则应用场景，有效解决制度执行中的模糊性问题。

4.2.1.2.1.4. 名词解释

针对公文起草、会议记录等场景中的专业术语、缩略词及政策新词，提供权威定义与扩展说明。系统支持相关制度关联及跨场景引用，帮助用户快速理解术语内涵，避免因概念混淆导致的沟通障碍或文本错误。

4.2.1.2.2. 智能搜索

4.2.1.2.2.1. 文档搜索

1.关键词搜索

通过关键词对文档进行检索，搜索文件标题或正文，支持查看搜索结果全文，查看时关键词高亮显示。支持选择搜索范围，全局或分库。

2.以文搜文

支持上传文档，自动分析文档内容，系统匹配相似文档：

查看发文原文：根据上级发文的文号、发文单位、原文，查询系统中被收录原文。

一致性评估：通过以文搜索，查看相关公文中相关提法前后是否一致、上下是否一致等。

系统支持 doc、docx、PDF、OFD、jpg、jpeg、wps、wpt 格式的文档上传。

4.2.1.2.2.2. 知识搜索

提供多维度查询，通过条件筛选快速、准确地找到所需要的知识。通过公文类型、公文主题、发文时间、发文部门、紧急程度、公文密级等多个维度进行分类，分类维度需从公文元数据中进行定义。这样可以快速定位公文范围，帮助用户快速查到所搜索的相关内容。

利用系统对电子公文的多维度标引，实现文档的多维度筛选，可对筛选维度进行管理与配置，帮助用户快速定位所搜索的相关内容，提高搜索准确度及搜索效率。

类型索引：支持根据公文类型查询相关公文。包括：命令、决定、决议、指示、公告、布告、通告、通知、通报、报告、请示、批复、函、会议纪要等。

主题索引：支持根据公文主题进行筛选，包括：政治、经济、文化、党建、社会、生态、国防等。

时间索引：支持根据公文发文时间进行筛选，用户可通过时间维度进行公文内容索引，快速定位公文位置。

发文部门索引：支持根据发文部门筛选，用户可通过发文部门进行公文搜索。

紧急程度索引：支持根据公文紧急程度进行索引，包括：特提、特急、加急、平稳等，用户可进行快速索引。

4.2.1.2.2.3. 文件智能阅读

自动提取文件中的关键信息（如标题、发文单位、政策要点），并以结构化形式展示，辅助用户快速掌握文件核心内容。在线阅读文档支持翻页、放大缩小、旋转、切换视图等，可收藏文档到个人收藏夹，根据权限也可进行下载和打印。

4.2.1.2.2.4. 相关文件推荐

1.在线阅读

提供无插件阅读，实现电子公文原版原式的在线预览，且可实现申请修正、下载等操作，根据权限可采取权限控制、分页授权等安全管控，实现在线阅读和安全阅读。

支持翻页、放大缩小、旋转、切换视图、打印、收藏文档等功能。

阅读界面展示公文标题、发文机关、成文日期、发布日期等元数据、公文的摘要、附件、关键词指数、高频词、分类标签、实体标引、系列文件、相关文件、所属文库等信息。

附件按照公文中的附件数量进行展示，支持对附件进行预览和下载。

2. 关联阅读

支持对电子公文的智能关联阅读，利用知识关联，快速关联人名/地名/机构名/文件名/会议/专业术语等内容，提高阅读效率和知识拓展。支持根据文档主题进行关联阅读。

4.2.1.2.3. 公文审校

4.2.1.2.3.1. 智能校对

提供文本校对智能应用服务能力。支持政治类、知识类、文字类、不规范类及自定义错误类型的文本校对内容的识别，提供识别内容的处置操作，包括替换，忽略，全部替换并查看。写作完成后进行校对，对文章进行扫描，将疑似错误的进行统计和呈现，并给出建议正确答案，由用户逐条核对是否进行替换，以此来完成文章的校对，确保所写文章没有基础性错误。

公文辅助 AI 系统与嵌入 AI 校对引擎，可对电子公文全文进行扫描和智能校对，从而大大降低错误率。可纠错类型如下：

（1）政治性错误：领导人姓名、职务、排序；台湾问题；反腐、涉黄涉暴、宗

教等；

（2）知识性错误：词条、人名、地名、科学常识等；

（3）文字类错误：拼音类、字形类、成语错误、多字少字、词语搭配、异形词等；

（4）不规范错误：英文拼写、数字/时间、计量单位、混合词等。

用户可对正在写作的文件进行校对，也可通过上传文件的方式进行校对。系统将对整个公文全文进行扫描，将疑似错误陈列在文档右侧，并展现统计数据“全部错误数量”“字词错误”“标点错误”“政治错误”。

4.2.1.2.3.2. 智能对比

支持上传两个文档进行对比，对比结果按新增、删除和更改三类变更展现。在公文辅助 AI 系统中，两篇待比较的公文被精确载入并并列展示，运用精密的文本分析算法，逐字逐句地剖析两篇公文的内容差异，准确反映了每一处具体变更，提升公文审核的效率和精确度，确保了所有增删改的异同点都被严格且无遗漏地识别，提升公文处理的严谨性和权威性。

（1）上传对比文档

通过上传两份文档进行对比，可上传 wps、wpt、doc、docx、PDF、OFD 等多种格式的文档。

（2）查看比对结果

用户完成比对文档上传后，系统将语义进行文档对比，并呈现比对结果，将原文与对比文档存在的差异进行统计，显示全部差异数量，新增内容数量、删除内容数量等，可直观地查看具体差异情况。

4.2.1.2.3.3. 合规性审查

系统内嵌了通用类政策文件以及合作区域特有的政策文件和详细解读，能够实时对各种类型的发文信息进行合规性校验或深入分析，支持对通用类政策文件库和本地合规审查专用手动维护和配置。支持基本信息合规性检查和正文内容合规性检查。

1、基本信息合规性检查

（1）标题要素逻辑性检查：检查公文标题中各机关单位的简称、全称；变更前

后的机构名称；机关单位根据行政级别进行先后顺序表述；标题文种使用规范性；审查 15 类公文文种以外的不规范文种描述；特殊公文标题符号使用规范性。

（2）发文字号：确认发文字号的格式是否符合规范（如“X〔年份〕X 号”），是否存在错误或遗漏。

（3）密级和紧急程度：确认公文是否正确标注了密级（如“机密”“绝密”）和紧急程度（如“特急”“加急”），并检查其标注位置是否符合要求。

（4）公文的主送机关、发文机关、印发机关、抄送机关等内容是否合规。

2、正文内容合规性检查

（1）政策合规性：通过系统内置的政策文件库和知识库，对公文中涉及的政策条款、法规引用进行合规性审查。检查引用的政策是否准确、是否为最新版本，是否存在与现行政策相悖的内容。

（2）正文要素完整性：正文引用文件规范性、附件标识；成文日期、印发日期年月份的完整性；成文日期、印发日期月份和日期不标虚位等。

（3）格式规范性：检查公文正文的段落格式（如首行缩进、行距、段落间距等）是否符合公文排版要求，检查各级标题的格式是否统一且符合规范。

4.2.1.2.3.4. 敏感信息筛查

每个用户单位根据自身情况创建敏感词库，如法律法规类、社会民生类、日常活动类、港澳台和领土/主权类、政策举措类、领导人类等，提供敏感词管理和敏感词设置，支持脱敏范围、处理方式设置，用于安全阅读和模型安全输出。可在每一个类别下可自主添加敏感词。系统也支持通过敏感词模板批量导入敏感词。通过部署敏感词动态云库以及语境用词场景的智能分析，有效实现了对各类发文内容中敏感词的精准筛查。

在创建敏感词库后，需对敏感词的应用范围进行配置。

1.添加敏感词方案，设置脱敏的使用范围，在组织架构中选择脱敏适用的用户对象，可按组织架构、角色进行脱敏范围选择

2.敏感词库选择，在已创建的敏感词库中进行选择脱敏词库，可单选、可多选，用户可设置脱敏元数据，可在元数据列表中选择元数据并进行脱敏。

3.敏感处理方式，可选择敏感词处理方式，如***替代，即以“*”代替敏感词，状态：敏感词方案可根据需要进行开启和关闭；编辑：用户可编辑敏感词方案，对原方案中的选项进行重新设置；删除：删除敏感词方案。

4.2.1.2.4. 智能写作

4.2.1.2.4.1. 生成全文

针对简单公文，公文辅助 AI 系统可直接生成全文。根据用户输入的主题或关键词，自动生成完整的文章内容。节省人工编写时间，同时确保公文内容的规范性和一致性。生成的公文还可根据实际需求进行个性化调整，如添加灵感、参考素材库选择等，实现不同场景下的生成全文一气呵成。

4.2.1.2.4.2. 生成大纲

用户根据需要输入标题，可生成提纲，根据标题或内容生成提纲后，生成的提纲若符合需求，可将生成的提纲插入到文档正文。插入到文档正文的提纲会自动调整为公文格式，符合公文写作要求，减少用户的操作。若生成的提纲不符合用户需求，则可选择“重新生成”，直至生成的提纲满意为止。

4.2.1.2.4.3. AI 仿写

公文辅助 AI 系统根据用户提供的原文，生成风格相似但内容不同的文本。提供多样化的表达方式和创意建议，生成符合不同场景需求的公文，对于重复性高、格式化的公文撰写任务，系统可以自动完成初稿生成和初步修改，显著减轻撰写者的工作负担。

4.2.1.2.4.4. 大纲润色

公文辅助 AI 系统根据用户需求生成大纲后，用户如果对大纲有不满意的地方，可选择“大纲润色”，将对大纲的通顺性、对称性等维度进行润色，使大纲更加对仗工整。润色后的大纲符合公文写作规范，还能提升公文的整体风格严肃性。

4.2.1.2.4.5. 添加灵感

在智能写作中，支持添加关键词作为灵感，系统会根据这些关键词，智能分析并生成与关键词相关的内容，快速构建公文的框架和要点。

4.2.1.2.4.6. 定向参考

在写作过程中，可参考指定的文件。公文辅助 AI 系统支持从本地上传和在库中选择文件两种方式进行参考，然后由大模型进行解析、参考和吸纳参考文件的观点，并纳入正在智能写作的文稿中，让写作内容更加符合用户的实际写作需求。支持在素材中多篇文档找到多个与描述词相关段落进行生成。生成的方式包括：

1.支持添加本地文件作为参考，将文件上传至个人公文库，并支持 ofd/pdf/doc/docx/wps/wpt 等格式文件。

2.支持添加公文库全库文件作为参考。

3.支持设定拟文单位和自定义设置输出字数长度进行条件参考。

4.2.1.2.4.7. 大纲成文

支持选择已经生成和修改后的大纲进行正文内容撰写，公文辅助 AI 系统将对大纲进行解析、上下文关联、意图分析，生成正文内容。大纲成文可确定“拟文单位”，还能进行字数限制。同时大纲成为还能参考指定文件，将指定文件中的关键信息和观点融入正文，确保内容的连贯性和准确性。

4.2.1.2.4.8. 内容润色

公文辅助 AI 系统支持对公文内容进行润色，让写作的内容更加结构化、书面化、逻辑化，以便于最终文稿可用于汇报、发表等公开场合。润色的过程不仅限于语言的优化，还包括对内容的深度加工，比如增强表达的严谨性、提升论证的说服力。系统自动识别并修正语法错误、拼写错误以及冗余的表达，同时保持原文的核心思想和意图不变。

4.2.1.2.4.9. 写作素材库

4.2.1.2.4.9.1. 模版库

模板库中公文类型包括行政公文或事务公文，界面展示相应的公文模板。通过关键词搜索方式，在模板库搜索框中，根据输入的关键词进行搜索匹配，查找对应的公文模板。可按类别查看模板列表，选择对应模板，进入编辑状态。

4.2.1.2.4.9.2. 范文样例

系统内置 15 个范文样例，用户可根据需求进行范文样例搜索。选择对应样例，

可将范文样例复制到编辑区域，用户仅需对部分内容进行修改即可完成文件撰写。

4.2.1.2.4.9.3. 素材库

素材库将用户参考库、公开参考库、专业参考库的文章进行碎片化处理后形成的素材库，用于写作时进行素材精准检索。通过材料库输入关键词搜索所需的素材内容，包括相关的素材推荐、法律法规、领导讲话等素材内容，可进行一键引用、复制、收藏等操作。

4.2.1.2.4.9.4. 文采库

文采库中主要是金句、成语、诗词等几类数据。可根据写作需求，在文采库中检索并选用合适的金句、成语或诗词，以增强文章的文采和表达效果。系统支持一键插入功能，将选中的文采内容直接嵌入到编辑区域中，使得写作过程更加高效便捷。

4.2.1.2.4.9.5. 我的素材

在我的素材中，提供素材筛选、管理、利用与数据同步等功能，支持复制我的素材内容，添加的素材插入至正文，可根据筛选标签对应显示素材内容，并通过后台对素材进行统一管理，通过同步机制保持我的素材与公文库-我的素材数据保持一致。

4.2.1.2.4.10. 公文续写

公文辅助 AI 系统自动联系提纲、上下文内容，对内容进行继续写，以便内容、字数更加充实，生成后续部分保持风格和逻辑连贯，在公文撰写过程中，系统基于已输入的提纲和上下文内容智能续写，保证生成的全文风格统一、逻辑严密。通过识别前文的主题、语气以及用词习惯，自动调整续写部分的语言风格，使之与整体文档保持一致。同时，系统支持对生成的文本进行实时的逻辑校验，确保各段落之间衔接自然，进一步提高公文撰写的效率和质量，减少因人工续写可能出现的错误和疏漏。

4.2.1.2.4.11. 重新拟文

当对生成全文结果不满意时，可通过重新拟文功能，对现有文档进行重写，生成全新的文本，满足不同场景的需求。重新拟文功能一是实现文本替换，二是深入理解文档的核心内容和意图，通过智能算法生成与原文档主题相同但表述方式、用词选择等方面不同维度的新文本。丰富公文撰写的思路，快速获得多样化的文本输出，同时保留了智能写作系统的高效性和准确性，确保生成的每一份新文档都经过严格的逻辑

校验和语言优化，达到专业公文的标准。

4.2.1.2.4.12. 公文排版

4.2.1.2.4.12.1. 常规公文排版

默认支持基于党政机关公文格式(GB/T9704—2012)对文本内容一键排版，系统将会对所写内容的标题、主送机关、大纲、正文、发文机关、成文日期进行一键排版，将检查行间距、字体、字号等格式内容，也可创建模板自定义排版。

1.格式自动化

根据公文类型（如通知、报告、请示等），自动套用相应的标准模板，确保格式规范。

自动设置标题层级（如一级标题、二级标题）、段落间距、缩进等段落与标题样式，符合公文格式要求。

自动设置正文字体（如仿宋体）、标题字体（如黑体）、字号（如正文三号字、标题二号字）等。字体与字号

2.页面布局

自动调整页边距（如上 3.7cm、下 3.5cm、左 2.8cm、右 2.6cm），符合公文标准的页边距设置。

自动添加页眉（如公文标题）和页脚（如页码），并确保页眉页脚格式统一。

自动处理分页控制，避免标题孤行或段落断裂。

3.编号与引用

支持公文中的条款、段落、图表等自动编号，确保编号格式统一。

自动处理公文中的引用内容（如法律法规、政策文件），并生成规范的引用格式。

4.附件排版

自动为附件添加标识（如“附件 1”“附件 2”），并设置附件标题格式。

附件分页：确保附件内容从新页开始，并与正文格式保持一致。

5..实时预览

所见即所得，提供实时预览功能，用户可随时查看排版效果，及时调整内容。

6.编辑与调整

支持手动调整，允许自定义排版模版，手动调整部分格式（如字体、段落间距），满足特殊需求。

4.2.1.2.4.12.2. 智能排版校验

依据内嵌的标准化公文模板，系统能够自动识别文件的种类，并据此进行套红处理，确保公文格式的规范性，支持上传本地常用的套红模板至系统，与预存的大量公文模板进行智能匹配，快速套用最符合的模板，提升查找以及文本处理效率，常用模版以列表形式呈现，一键套红实现快速生成符合规范要求的版面。套红过程中对可能出现的偏差支持自动调整和手动调整，对多种格式公文的套红校验。同时，该系统还能够对文件内容进行深入的校核，包括但不限于检查语病、错别字等基础性错误，辅助人工校验以减少时间成本提高公文内容准确性。

4.2.1.2.5. 智能填单

智能填单功能与执委会电子公文系统深度集成，实现文件填报流程的预处理，智能提取来文发文中 18 项公文元数据重要信息的能力，能够根据提取的内容生成抽取式摘要，从而提高文件处理的效率和准确性。

依据来文办件等执委会电子公文交换系统流程中的文件关键词，自动提取诸如标题、来文单位、文件来源、紧急程度、密级标识等关键基础元数据信息，提取的信息可直接以接口形式流转至执委会电子公文交换系统中的下一环节，提高公文流转效率。

4.2.1.2.6. 入库管理

4.2.1.2.6.1. 文档入库

支持不同来源，不同类型的文档资源，通过自动或手动上传方式文档入库，显示不同阶段包括全部、待人工处理、系统处理中、处理异常、待审核和已入库文档列表信息；支持文档入库不阶段的数据处理操作包括查看、编辑，重试，删除，添加位置等操作。

1.文档上传

针对个人电脑上的文件，可由用户手工上传电子公文文件进行入库。上传文件的同时，用户选择文件类型、入库方案、入库位置、是否添加附件等多个功能。

2.自动采集

通过 API 接口可从电子公文系统（OA）等业务系统中定时、自动、批量获取电子文件数据。公文辅助 AI 系统在获取到文件时，根据对应的入库类型、入库方案进行对应处理后直接入库。

3.文档列表

提供以列表形式展示入库文档，包括：

（1）列表默认展示内容；

（2）自定义列表展示内容；

（3）条件检索；

（4）展示列宽度自定义、根据用户习惯调整后再次进入保留调整后的样式。

4.2.1.2.6.2. 入库任务

入库任务的列表展示，内容包括列表默认展示内容和自定义列表展示内容，同时，还支持条件检索和展示列宽度自定义功能。

1.入库任务检索

通过方案类型、创建时间、上传文档来源及上传文档名称对入库任务进行筛选搜索，根据实际需求，选择相应的筛选条件，快速定位到目标入库任务。同时，系统还支持对筛选结果进行排序，如按创建时间升序或降序排列，以便用户更加直观地查看和管理入库任务。

2.查看入库任务

完成文件入库操作后，在入库任务栏目中，可查看入库进度，掌握哪些入库任务完成情况以及每个入库任务的详细信息和状态。提供任务进度条或百分比形式，展示入库任务的完成情况。对于需要审核的入库任务，提示审核人及审核状态，便于用户及时跟进和处理。若入库任务发生异常，系统会列出异常原因。

4.2.1.2.6.3. 入库方案执行

1.文件格式转换

（1）文件转换为 OFD 格式

入库的文件统一转换为 OFD 格式文件，以便长期保存。按照国家公文标准或内部公文标准，可将非标准格式的终稿的电子公文，包括：WPS、DOC、DOC、PDF、

JPG、JPEG、PNG、BMP、TIF、TIFF、CEB、CEBX、S92、GD 等多种格式转换为 OFD 格式进行存储。同时原格式文件不变，仅作存储，以便后续使用。

（2）扫描件双层 OFD 处理

系统通过识别到扫描件图片格式文件，启动 OCR 引擎，对图片类文件进行 OCR 文本识别，形成含有图片、文本的双层 OFD 文件。

（3）失败重试

文档入库，自动服务异常 ，可以通过手动触发，重新调用格式转换服务。

（4）删除文档

系统支持删除入库的文档。

（5）查看文档

入库展示文档内容详情，包括：ofd 格式的文档内容、文档提取信息（包括：元数据、基本信息、实体、敏感词、附件等），如果文档有拆分可查看拆分前的源文件、可查看拆分后的结果。

（6）手动拆分

系统支持人工对上传文档进行拆分，可自定义目录层级。

（7）自动拆分

系统支持根据子目录层级对上传文档自动进行拆分。

（8）查看拆分结果

系统支持拆分后查看拆分结果，也支持返回对文件进行重新拆分。

4.2.1.2.6.4. 文库管理

支持内置文库和自定义业务维度的文库管理和维护。提供文库的新建，重命名、设置管理员、权限设置、安全设置、删除等功能；目录的新建、重命名，移动、权限设置和删除等功能。

（1）新建库

系统提供新建文库功能，支持创建模板库、范文样例库，支持文库自定义排序、对文库分类增加注释，便于用户管理、使用。

（2）展示文库列表

系统提供对文库列表的展示，支持文库按分类管理、展示，展示已有文库名称、类型、所有者、文库文件数量、文库类型。

在系统中可进行表头配置，包括：默认展示列、可配置哪些扩展列、哪些列不可删除。

（3）查看文库详情

查看文库内目录及文档信息，可根据文档名称、文档来源、操作人、文档类型、元数据对文库文档进行搜索。

（4）设置库权限

设置库范围内文档的前台查看、复制、打印、下载等权限。

支持按照租户、单位、部门范围配置，根据配置范围展示审核人可选范围。

（5）设置管理员

设置库的后台管理员，支持按照租户、单位、部门范围配置，根据配置范围展示审核人可选范围。

（6）库重命名

支持对文库名称进行修改。

（7）转移所有权

系统支持设置文库负责人。

（8）安全设置

设置文库脱敏规则、是否开启水印。

（9）是否前台展示

设置文库是否在前台展示。

（10）删除文库

系统提供删除库功能，仅允许删除空库。

（11）库的检索条件配置

设置前台可展示哪些文库检索条件，包括：分类标签、文档类型、目录等。

（12）库的表头配置

设置文库在前台展示的具体列表项。

4.2.1.2.7. 文档管理

通过文库和目录查看和管理系统内的文档，查看文档基本信息，阅读文档内容，移动文档位置。查看和修改文档的标签信息，设置用户对文档的操作权限。

1.设置文档权限

设置某具体文档的前台查看、复制、打印、下载等权限，针对不同用户角色设置不同的操作权限，确保文档的安全性和合规性。

2.移除文档

支持将文档从该文库中移除，当前文库中不可见，支持文档的重新分类或临时隐藏，移除后的文档可通过系统后台进行恢复或重新分配至其他文库。

3.查看文档详情

展示文档基本信息、元数据提取信息、标签提取信息、附件信息、过程文档、敏感词信息。

4.文档在线阅读

展示文档详情，阅读展示内容包括但不限于文档的标题、作者、创建日期、修改日期等基本信息，利用轻阅读能力，如打印、页面调整、缩放等功能，提高阅读效率和体验。

5.移动文档

调整文档所在目录位置，用户可将文档从一个目录移动到另一个目录，便于文档的分类管理和快速查找。通过简单的拖拽操作或选择目标目录进行移动，系统将自动更新文档的路径信息，确保文档链接的有效性。

6.下载文档

下载文档及其附件，查看预览目前仅支持轻阅读能打开的类型，其他格式需下载到本地查看。点击下载按钮系统将自动处理下载请求，将文档及其附件保存到用户指定的本地位置。提供下载进度条，实时显示下载进度，以列表形式展示下载历史记录，用户可查看和管理自己的下载记录，方便后续查阅和使用。

7.编辑文档

提供设置文档的元数据信息、标签信息等功能。支持对文档进行标签信息调整，

包括添加分类标签、删除分类标签、添加关键词标签、删除关键词标签、添加实体标签、删除实体标签。

8.修改封面

支持对文档封面进行修改替换，用户可根据需求，自定义文档的封面设计，提升文档的分类和标签性，支持上传自定义图片作为封面，实现个性化设置。点击修改封面按钮，即可完成封面的替换。

4.2.1.2.8. 配置管理

4.2.1.2.8.1. 文档入库配置

文件入库前，须配置入库方案，即对文件入库位置、处理方式、审核机制等内容进行设置，当文件入库时，系统则自动按照入库方案进行标准化处理。支持自定义入库方案配置，用于不同类型文档入库后的数据处理。节点配置项包括格式转换、文字识别、文件拆分、信息提取、人工处理，审批等。

1.对入库文档所需要涉及的流程进行定制化配置，并指定方案可生效的文档类型；

2.支持修改入库流程配置信息，对入库方案进行修改，删除入库方案，删除不再使用的入库方案；

3.系统支持展示所有入库方案；同时还支持按条件检索，对列表中的入库方案进行删除、修改，启用/停用等操作。

4.支持设置入库方案状态，启用的入库方案能够在文档入库时被选择。

4.2.1.2.8.2. 基础数据配置

提供文档类型、元数据和标签等业务资源配置管理，用于支持不同维度的文档入库与展示。在基础数据配置中，用户可自由定义和配置文档类型，包括但不限于函件、报告、计划、总结等多种文档格式，以满足不同业务需求，支持对每种文档类型设置专属的元数据字段。

4.2.1.2.9. 安全管理

4.2.1.2.9.1. 权限管理

提供角色维护与管理，支持按角色进行权限设置，包括功能权限和数据权限的设置。角色设置灵活多样，可以针对不同的岗位或职责创建角色，并为每个角色分配相

应的功能权限，确保用户只能访问和操作其职责范围内的系统功能。文件权限的设置则更为精细，可以控制用户对特定数据或文档集的访问权限，有效保护敏感信息，防止数据泄露。通过角色与权限的绑定，系统能够自动根据用户的角色分配相应的权限，简化权限管理的复杂性，提高管理效率。

数据权限是在租户范围内，管理业务模块的用户数据权限，包含支持在列表中查看本人数据、本部门（及下级）数据、本单位（及下级）数据权限

4.2.1.2.9.2. 日志管理

提供用户登陆和操作日志审计功能，支持日志信息按模块，账户，状态和时间段检索和导出功能。可支持三员日志审计。日志管理功能详细记录了用户在系统中的操作行为，包括登录时间、操作模块、操作账户、操作状态以及操作时间段等关键信息。系统支持用户根据特定需求，对这些日志信息进行精细化的检索。用户可以选择按模块检索，快速定位到特定功能模块的操作日志；或者按账户检索，查看某一用户账户的全部操作记录。同时，系统还支持按状态和时间段进行检索，帮助用户筛选出特定条件下的日志信息。日志管理功能支持日志导出功能，用户可以将检索到的日志信息导出为 Excel 或其他格式的文件，便于后续的分析和处理。

4.2.1.2.10. 安全控制

4.2.1.2.10.1. 系统安全

4.2.1.2.10.1.1. 安全存储

政务大模型底层存储设施，采用去中心化的分布式对象存储进行持久化保存，并利用多副本机制进行冗余保存，可有效抵御数据中心的数据损毁。在存储安全部分引用数据备份保障机制，提供了全量、增量等多种备份策略，最大限度地保证数据安全。

针对涉密文件或重要敏感文件，可对接加密机进行加密存储。

4.2.1.2.10.1.2. 安全传输

在数据传输过程中设计采用支持密文及密钥的 https 协议进行传输，尽可能地保证信息在传输过程中不被截获、篡改，并利用统一身份认证平台，确保使用者的身份，结合支持国密算法的加密设备进行文件的加密传输，保障通信安全。

4.2.1.2.10.1.3. 安全运维

基于信创基础资源为底座，采用国产基础软硬件构建的同时，结合国标 OFD 的安全能力，为政务大模型的安全运转提供安全保障。

4.2.1.2.10.2. 文档安全

4.2.1.2.10.2.1. 安全阅读

采用终端无缓存机制，对文件进行切分、按需传送，使文件不落地、快速加载，本地不留缓存文件。支持文档水印和动态水印（即运行时水印）：可通过接口传参设置文字水印内容及显示样式，支持水印的打印及显示控制，同时可控制打印份数、红黑章效果。可全面记录用户登录、阅读、下载、打印、复制等操作行为。

4.2.1.2.10.2.2. 安全检索

采用分库存储，所以检索时，可根据需要到相应的库中进行检索需要的内容，如：关键词、元数据等，而无需再通过原文库去搜索，无需多次打开原文进行检索，减少了原文被破坏的可能。同时，检索行为可纳入权限管控及操作日志，便于系统安全审计。

4.2.1.2.11. 系统管理

4.2.1.2.11.1. 菜单管理

支持对系统功能菜单进行维护，包括添加、删除、修改菜单项，以及设置菜单项的访问权限，确保不同角色的用户只能访问其权限范围内的功能菜单，提高系统的安全性和易用性。

4.2.1.2.11.2. 字典管理

支持对枚举值等字典项进行维护，包括添加、修改、删除等操作。通过字典管理，系统管理员可以方便地管理系统中使用的各种枚举值，如状态码、类别码等，确保数据的准确性和一致性。同时，字典管理还支持导入和导出功能，方便管理员在不同系统间迁移或备份字典数据。

4.2.1.2.11.3. 参数设置

支持对系统参数进行设置，通过参数设置模块，包括但不限于系统时区、日期格式、语言选项等，以满足不同用户特定需求。参数设置模块支持管理员浏览、修改和

保存参数配置，提升系统的灵活性和适应性。

4.2.1.2.11.4. 授权信息查看

（1）授权信息查看

查看用户授权策略，展示对接的授权中心信息，包括授权数量、有效期。以及授权状态等关键信息，帮助系统管理员全面了解用户授权情况，确保系统的授权管理规范有序。同时，该功能还支持导出授权信息，方便管理员进行审计和备份。

（2）授权信息查看

支持查看该租户下授权基本信息，包括授权的类型、授权级别、授权时间等详细信息，帮助系统管理员深入了解租户授权情况，确保授权的准确性和合规性。此外，该功能还提供了筛选和排序功能，管理员可以根据需要快速定位到特定的授权信息，提高工作效率。

（3）授权对接

对接授权中心获取授权指令。

4.2.1.2.12. 本地化语料库建设

1.收集合作区成立以来所有历史公文数据（其中收文 15 万件、发文 5 万件，存量公文数据约 3T），按文种（通知、报告、函）、主题（金融、民生、跨境合作）分类；

2. 建立语料库实现公文数据的存储、检索和分析功能，方便用户快速查找和利用相关公文信息。定期对语料库的功能进行更新和维护，确保合作区公文处理工作的需要；

3.基于合作区政策文件、历史公文库、粤澳跨境协作案例，构建专属语料库，强化模型对“横琴特色”内容的生成能力。该语料库不仅涵盖合作区的政策文件，还包括历史公文库和粤澳跨境协作案例，确保模型能够深入理解“横琴特色”的语境和背景。

4.智能公文能处理的数据范围是公文类，主要为 15 类行政公文，且不包括表格、工程文件、PPT。

4.2.1.2.13. 系统前端界面建设

4.2.1.2.13.1. UI 配置

公文辅助 AI 系统的功能模块 UI 配置符合 OA 办公流程，支持前台首页页面布局的配置，包括数据源、属性和关系的配置；支持外观包括主题、LOGO、背景等设置，可灵活调整首页的展示内容和风格，以适应不同的系统界面或业务展示需求。通过适配主流浏览器前端设计标准，确保智能公文模型在各种环境下都能稳定运行。设计步骤如下：

1.需求分析与规划，分析 OA 办公流程中公文处理的具体需求，明确智能公文模型的功能目标。与业务部门沟通，确定 UI 配置的核心功能和用户体验目标。注重前端界面的简洁性和直观性，确保用户能够快速上手并高效操作。

2.根据 OA 系统的整体风格，设计智能公文模型的页面布局，确保界面简洁、直观。优化操作流程，设计符合用户习惯的交互逻辑，减少操作步骤，提高效率。在页面色彩搭配上，采用与 OA 系统相协调的色调，贴合 OA 进行图标和按钮的设计，提升用户的操作体验。

3.确保功能模块清晰易用。集成智能辅助功能（如一键排版、智能校对等）的交互设计，提升用户体验。在功能模块布局上，公文起草、撰写、校对和修改等关键流程被置于显眼位置，用户能够快速找到所需功能。在交互设计上，考虑用户原有的使用习惯和反馈，通过不断的迭代和优化，使功能模块更加符合用户实际办理需求。例如，在公文撰写模块中，提供了丰富的模板库和素材库，用户可以根据自己的需要选择合适的模板和素材，快速完成公文撰写。

4.对主流浏览器进行适配，确保界面在各种环境下都能正常显示。并进行用户测试，收集反馈意见，优化界面设计和操作流程，对于不同分辨率和屏幕尺寸的设备，系统能够自动调整布局和元素大小，保证界面元素的清晰度和可读性。

4.2.1.2.13.2. 首页门户

提供系统首页内容展示；支持基于可视化配置门户页面，首页分为三大入口，即主题库入口、智能应用入口、智能推送入口。

1.主题库入口主要展示用户业务数据（工作）、权威参考数据（参考）。

工作库是指用户自行上传的公文档案、会议材料、政策法规、领导讲话稿、简报、期刊等内部高价值文件，当让用户选择工作库入口，则可直接进入工作库，根据用户权限，并可进行检索或对应内容查看。

参考库是通过对国家部委、人民政府、权威媒体等机构官方网站进行定向采集整理入库的公开、无版权的数据内容，主要是总书记重要讲话、工作报告、法律法规、政策文件、党纪法规、信息公开等类型的文件，参考库内的信息一般默认无权限限制

2.智能应用入口主要展示智能搜索、智能问答、智能写作、智能比对、智能校对、智能查重智能应用入口。

3.智能推送入口主要展示近期热文、领导讲话、个性推荐等系统推荐内容。

根据浏览量推荐热点文章，展示国家领导人近期重要讲话的内容链接，根据用户历史的搜索和浏览信息，推荐并展示用户可能关心的其他相关文档。

4.2.1.2.13.3. 个人中心

显示个人工作信息，包括支持显示个人信息、历史浏览、收藏夹。

1.个人信息展示个人基本信息，主要包括用户姓名、登录名、邮箱、组织架构等内容，支持在个人中心修改登录密码，修改后原密码失效，需使用新密码重新登录。

2.历史浏览支持查看自己搜索和浏览文档的历史记录。

3.收藏文件以列表方式展示当前账号的收藏文档，可通过文档名称及收藏时间进行搜索。支持管理自己收藏的文件，进行取消收藏操作。

4.2.1.2.13.4. 数据统计

提供系统内不同维度的数据资源信息，包括文档数据总量、访问统计、文档类型统计、入库趋势、文档标签统计等。

展示公文辅助 AI 系统的统计数据，随时掌握系统内文档类型统计、文档数据总量、入库趋势、文档标签统计、日访问量统计、热搜词汇、热点信息等数据，通过热点文章、热搜词汇、文档数量、文档浏览量等，从电子公文的深度视角反映本单位当前的使用状态。

1.单位文档贡献统计，展示上传到公文辅助 AI 系统中的公文数量，可以按本周、本月、本年度等维度进行统计。

2.文档数量统计，展示公文辅助 AI 系统里的累计总文档数量，包括手动入库总数、自动入库总数、本月新入库文档数、今日新入库文档数。

3.日访问量统计，展示用户每天访问系统的情况，可以按本周、本月、本年度等维度进行统计。

4.文库数量统计，展示公文辅助 AI 系统中的文库总量、公开文库量、内部文库量。

5.文档浏览量统计，展示文档浏览量的统计信息，可以按本周、本月、本年度等维度进行统计。

6.分类入库排名，展示不同分类的文档入库排名，可以按本周、本月、本年度等维度进行统计。

7.知识库文档统计，展示知识库文档统计信息，包括知识库文档总量、片段素材总量。

8.热搜词汇，展示用户常搜的词汇信息，可以按本周、本月、本年度等维度进行统计。热搜词汇反映了用户的关注热点和需求趋势，有助于管理员了解用户偏好，优化系统内容推荐，提升用户体验。同时，热搜词汇的统计也为文档分类、标签设置等提供了数据支持，有助于进一步提升系统的智能化水平。

9.热点信息，展示用户经常阅读的热点文章，可以按本周、本月、本年度等维度进行统计。

4.2.1.2.13.5. 我的文库

1.展示上传文件，可上传文件至我的文库并添加分类。

2.删除文件，可对我的文库文件进行删除。

3.查看文件详情，支持通过 web office/轻阅读查看文件，流式文件支持编辑。

4.移动文件，支持将文件移动至其他目录。

5.目录管理，系统支持新建目录、修改目录、删除目录。

6.文件检索，可通过文档编号、文档名称、分类检索文件。

7.提交入库，将文档依据后台入库逻辑入库。

8.我的素材

（1）添加素材，在文档阅读页通过右键菜单添加素材。

（2）删除素材，系统支持删除素材。

（3）素材标签管理，可指定素材分类及标签。

（4）素材检索，支持通过素材内容、类型、标签搜索素材。

4.2.1.2.13.6. 标签管理

（1）标签列表

按标签类别展示分类标签，支持查看标签的子分类，支持分类名称检索。支持对分类标签操作，包括新建子分类、重命名子分类、删除子分类等功能。同时还支持展示列表的自定义排序。

（2）新建分类

支持批量创建分类标签。

（3）重命名分类标签

支持对分类名称进行修改。

（4）新建子分类

在选择上级分类下新建子分类。

（5）删除分类标签

将分类标签及分类下子分类一并删除。

（6）导入分类标签

通过导入数据表格批量新建分类标签。

（7）导出分类标签

通过表格导出当前列表全部标签。

（8）初始化分类标签

初始化内置文库数据所需标签、辅助写作所需标签，满足模板库、范文样例库的使用需求。

4.2.1.2.13.7. 组织架构管理

系统支持对各单位的组织架构进行创建和管理。包括新建机构、删除机构、修改组织架构、移动。

租户管理：租户单位指的是在使用电子文件库系统时，必须事先注册并获得系统

管理员授权的单位或组织。这些单位在系统内拥有专属的账户和权限，能够自主地执行电子公文的创建、发送、接收、存储等操作。当下级单位进行独立管理时，系统新增了添加租户的功能。可以为每个单位进行个性化设置。在租户单位中，能够实现库内文件数据的隔离，确保各单位文件的安全性。

4.2.1.2.13.8. 用户管理

1.创建用户，填写用户相关信息，具体如下：

序号	字段名称	字段要求	备注
1	登录名	字符填写	
2	密码	字符填写	
3	姓名	字符填写	
4	性别	下拉选项	男/女
5	手机号	字符填写	
6	归属部门	下拉选项	
7	角色	下拉选项	
8	邮箱	字符填写	
9	排序	字符填写	
10	备注	字符填写	

2.导入用户

通过导入数据表格批量新增用户。

3.导出用户

通过表格将当前选择部门用户导出至本地。

4.信息修改

可对已创建的用户信息进行修改。

5.启用/禁用账号

系统管理员可对用户的状态进行设定，启用或关闭。

6.启用/禁用 WPS 端

系统管理员可对 WPS 端的用户状态进行设定，启用或关闭。

7.重置密码

当用户在使用政务大模型时，存在忘记密码的情况，管理员可对用户的密码进行重置。

8.批量操作

对用户进行批量操作，包括批量启用账号、批量禁用账号、批量删除用户。

9.用户列表

显示用户列表，支持按条件检索用户。

10.用户账号对接接口

支持以接口形式对接第三方系统的用户账号信息。

4.2.1.3. 系统对接

4.2.1.3.1. 本地 WPS 客户端插件

基于行政事务局已采购的 WPS 客户端，提供公文辅助 AI 系统拟建设的辅助写作能力，包括智能写作、智能校对、智能排版，智能查重、智能对比等能力。

4.2.1.3.1.1. 用户登录

用户可在 WPS 客户端输入账号密码，登录公文辅助 AI 系统。

4.2.1.3.1.2. 资源库

1.公文模版，用户可在 WPS 客户端中选择事务公文和法定公文模板，可对模板进行搜索，点击可查看模板详情进行预览，并支持将模板导入写作界面应用相关模板。

2.范文样例，在资源库中根据公文类型筛选、查找相关范文样例，可自动识别文档标题作为搜索条件，通过列表进行结果展示。支持查看范文详情，阅读范文样例全文内容，将范文样例插入编辑页面。

3.素材库允许用户自动识别文档标题作为搜索条件，快速定位所需内容。用户可以从总书记重要讲话、政策文件、法律法规三个文库中选择，或者自定义关键词进行搜索。搜索结果将基于搜索条件和用户设定的筛选分类条件进行展示，确保用户能够精准地找到所需素材。用户可预览查看材料的原文，还可以选择将选定的素材直接插入至文档编辑区，或者将其添加至系统剪贴板，方便后续的复制和使用。此外，系统还支持用户对单条素材进行收藏或取消收藏操作。

4.文采库提供了丰富的金句、成语和诗词资源，用户可以根据自己的需求进行自定义的关键词搜索。通过筛选分类条件对结果列表进行精确筛选，快地找到满足需求的素材。搜索结果将基于用户的搜索条件和筛选条件进行展示，确保用户能够轻松找到与需求相关的文采素材。对于成语和诗词，文采库还提供了详细的详情查看功能，

让用户能够深入了解其含义、来源和用法。用户可以将选中的素材直接插入至文档编辑区，方便在文档中使用。文采库支持将素材添加至系统剪贴板，方便用户在其他应用程序中快速粘贴和使用。支持对单条素材进行收藏或取消收藏操作，以便日后快速访问。

4.2.1.3.1.3. 保存至我的文库

写作过程中将撰写的文稿保存到 WEB 端“我的文库”中，可在 WPS 客户端和 WEB 端分别进行查看。

4.2.1.3.1.4. 文档入库

在完成文稿写作后，可在 WPS 客户端直接提交入库，即文稿将被上传至指定的共享文库内。上传文件的文档类型、所属租户、入库方案均需进行配置，支持添加附件，完成入库操作后，由系统直接对文件进行一系列标准化处理。

4.2.1.3.1.5. 智能查重插件

在 WPS 客户端可使用智能查重功能，与指定库内的文件进行查重对比。

4.2.1.3.1.6. 智能对比插件

在 WPS 客户端可使用智能查重功能，与指定库内的文件进行查重对比。

4.2.1.3.1.7. 智能校对插件

在 WPS 客户端，可直接调用智能校对引擎对所写文稿完成校对。

4.2.1.3.2. 业务认证及权限对接

4.2.1.3.2.1. 文件权限管理

支持用户分级分权管理和数据分级分权控制，实现用户-部门-文档权限的联动管理，用户的数据访问权限仅限所属部门相关数据，并支持管理员在后台实现应用权限和数据权限的灵活配置。

1.根据合作区部门架构及公文密级（公开/内部/机密），设计“部门-角色-文件”三级权限模型，保障数据主权（私有化部署）、权限分级管控（涉密文件隔离），确保符合内部管理要求；

2. 对系统公文文件进行隔离存储与访问控制，确保机密文件不被非授权用户获取；

3. 提供详细的权限审计日志，记录用户对文件的访问和操作行为，包括但不限于

文件的创建、修改、删除、查阅、下载等，确保每一次权限使用都有迹可循，便于后续的安全审计和追溯。

4.开发动态权限分配功能，支持临时授权（如跨部门协作时向指定人员开放文件编辑权限）。

5.集成智能权限提醒机制，当用户尝试执行超出其权限范围的操作时，系统自动弹出权限不足提示，并引导用户申请所需权限或联系管理员，提升用户体验和权限管理的透明度。

6.实现权限变更通知功能，每当用户的权限发生调整，无论是新增、修改还是撤销，系统都会即时通过邮件或站内通知的方式告知用户，确保每位用户都能及时了解自己的权限状态。

4.2.1.3.2.2. OA 接口联调

1.完成大模型与现有一个 OA 系统的 API 对接，实现公文辅助 AI 系统与现有 OA 系统、电子政务平台无缝对接，打通数据孤岛，确保权限、流程、安全体系与单位现有架构一致；

2.基于当前 OA 系统环境，提供灵活的适配方案，确保接口的稳定性和数据的准确性，减少因系统升级带来的对接障碍；

3.建立数据校验机制，确保在数据同步过程中数据的完整性和一致性，避免因数据错误导致的业务中断或流程异常；

4.提供详细的接口文档和操作指南，方便单位 IT 人员进行日常维护和故障排查，降低运维成本。

4.2.1.3.2.3. 单点登录

集成内部统一身份认证系统（或文件管理权限体系），支持员工通过 OA 账号一键登录智能写作平台。开发单点登录功能，包括用户认证、令牌生成与管理。集成 OAuth2.0 标准协议，实现用户在两个系统间的无缝切换。实现单点登录拦截器和资源服务器。同时，为了确保单点登录的安全性，我们采用加密传输和严格的身份验证机制，防止未授权访问。此外，我们提供详细的单点登录日志记录，便于追踪和审计用户登录行为，及时发现并处理潜在的安全风险，实现用户一次认证即可访问多个系统

（如 OA 系统、智能写作工具等），减少重复登录的繁琐操作，减少系统间的身份认证障碍。

第五章 系统业务运营服务

5.1. 业务管理运营服务

确保数据在 OA 系统与人工智能办公系统之间高效、准确地传输，提供稳定的接口性能，支持高并发操作，确保系统运行流畅，实现功能模块的深度集成。

5.1.1. 业务场景运营

5.1.1.1. 问答场景优化

（1）提升问题识别准确率与答案覆盖率

通过梳理行业知识体系与用户高频问题场景，对现有知识库进行语义化重构与多维度标签分类，强化同义词映射、上下文关联及歧义消解能力。同步建立“用户提问-答案采纳率”回溯机制，通过未命中问题归因分析持续补充知识盲区，辅以人工专家团队双周巡检校准，保障核心场景应答准确率不低于 90%。

（2）实现 10 秒内平均响应时效

基于智能路由与算力资源弹性调度，构建分级响应体系：高频标准化问题由 AI 引擎优先触发预置答案库毫秒级响应。

本阶段工作预计投入 4 人月，费用约 6 万。

5.1.1.2. 审校场景优化

（1）用户需求调研

目标用户访谈，通过与合作区内意见领袖和目标用户进行深度访谈，了解其校对和公文对比的具体需求。

场景化分析用户在不同场景下的使用习惯和痛点（如公文起草、审核、归档等）。

（2）数据采集与优化

建设校对语料库，收集大量公文校对样本和校对范本，涵盖不同行业和场景，确保语料库的多样性和代表性。

对语料进行人工调优或校对数据库偏好设置，包括错别字、语法错误、格式问题等，为智能校对提供标准参考数据。

（3）校对审核测试

收集反馈并优化功能设计，通过实际校对测试，收集用户对智能校对系统的反馈意见，包括但不限于校对准确性、效率、易用性等方面的评价，针对用户反馈的问题和不足，对系统功能设计进行优化调整，以提升校对效果和用户体验。

（4）规则库构建与优化

基于公文写作规范，制定错别字、语法、标点等校对规则；制定公文内容对比的规则（如段落对比、表格对比、附件对比等）。

分析用户提交的错误数据，优化校对规则和对比算法，定期更新校对和对比模型，提升系统的准确性和适应性。

确保调研覆盖 80%以上的目标用户群体，标注准确率达到 95%以上，通过原型测试，确保用户对功能设计的满意度达到 90%以上。

本阶段工作预计投入 6 人月，费用约 9 万。

5.1.1.3. 写作场景定制

（1）用户调研

针对不同岗位、部门的公文写作用户，了解其日常写作痛点、对现有工具的使用感受以及对新功能的期望。通过线上问卷平台、线下访谈等方式收集数据。组织焦点小组讨论公文写作场景，如合作区会议纪要、报告撰写等公文写作特点。

（2）本地写作模版配置

预置合作区常用公文模板（如请示、函、纪要、报告）15 个，支持自定义模板库管理；

对于特殊格式或内容要求的公文，智能写作工具提供定制模板开发设计服务。政府工作人员提出定制需求后，运营人员会与需求方深入沟通，详细了解公文的应用场景、格式规范以及内容侧重点，根据公务人员业务需求和参考样例文件新增定制模板。

（3）特殊文种写作应用优化（非常规行政事务公文）

针对合作区内出现的特殊文种，属于非常规行政事务公文，智能写作工具将进行优化，定期分析用户使用智能写作应用的反馈，识别常见问题和需求，优化生成特定 AI 非常规公文模版 10 个。

本阶段工作预计投入 4 人月，费用约 6 万。

5.1.2. 系统技术运营

5.1.2.1. 模型反馈机制建立

多维度评估体系搭建。定义核心评估指标，公文格式合规率、政策引用准确率、问答意图匹配度、素材推荐点击率等，构建量化评分模型；每月生成《模型效能分析报告》共约 12 份，结合用户反馈数据与系统日志，定位模型薄弱环节，明确优化优先级。

本阶段工作预计投入 3 人月，费用约 4.5 万。

5.1.2.2. 模型优化

根据评估结果，定期列出优化措施、优化效果及下一步优化计划，确保公务人员能够清晰了解模型优化的进展和成果。实现模型与与业务场景的深度融合，优化模型的使用效果。

本阶段工作预计投入 10 人月，费用约 15 万。

5.1.3. 管理支撑运营

5.1.3.1. 用户与权限管理运营

从电子公文系统获取公务人员变动信息，如人员新增入职、人员岗位调动或离职等，及时对用户账号进行相应处理，包括账号的创建、权限的调整以及离职账号的禁用等，确保用户账号信息与政府内部人事信息的实时一致性。同时，对于因业务需要而临时访问系统的外部人员，提供临时账号的申请、审批及到期自动回收服务，保障系统安全的同时满足业务需求。

（1）对于新增人员，依据其所在部门、岗位职能以及工作权限，在行政办公大模型平台上创建对应的用户账号。在创建过程中，按照预先设定的账号权限模板，为新账号分配合适的权限，确保其能够访问和使用与工作相关的功能模块和数据资源，如起草特定类型公文、查询相关公文资料等权限。同时，通过系统自动发送系统使用手册及使用指引，引导公务人员尽快登录平台熟悉操作。

（2）当员工发生岗位调动时，根据新岗位的职责和权限要求，对其用户账号的权限进行相应修改。例如，公务人员岗位调动时，其可访问的公文类别、可使用的功

能模块可能会发生变化，及时调整账号权限，保证公务人员能够正常开展新岗位工作。

（3）对于离职人员，一旦收到离职通知，系统将立即禁用其账号，防止离职人员继续访问系统。同时，系统会记录离职账号的禁用时间，以备后续审计或查询需要。在禁用账号前，系统会检查该账号是否有未完成的公文处理任务，确保业务连续性不受影响。

本阶段工作预计投入 1 人月，费用约 1.5 万。

5.1.3.2. 需求收集与反馈

（1）用户调研

面向局内办公室、编办等高频公文公务场景中的用户，以问卷调查方式设计针对公文处理需求的问卷，收集用户反馈；与典型用户进行一对一访谈，深入了解具体需求，实地观察用户使用系统的场景，记录使用中的问题。

（2）数据分析

前期通过系统日志收集用户使用数据，发现用户潜在需求和功能改进点。后期采用沟通群或规范文档记录需求和问题。

（3）需求整理与优先级排序

将收集到的需求按功能模块（如智能审校、智能问答、智能写作等）进行分类。根据需求的重要性和紧急程度，制定需求实现的优先级。

（4）反馈处理

将用户反馈按问题类型（如功能问题、性能问题、体验问题等）进行分类。根据问题类型，分派给技术支持、产品经理或开发团队进行处理。持续跟踪问题处理进度，确保用户反馈得到及时响应。

（5）数据分析与改进

定期分析用户反馈数据，发现共性问题和高频需求，根据反馈数据，优化系统功能和用户体验，并将典型问题和解决方案整理成案例，供用户参考。

本阶段工作预计投入 2 人，持续工作 2 个月，预计工作量 4 人月，费用约 6 万。

5.1.3.3. 系统推广与培训

（1）宣传与推广活动

面向全局组织宣贯交流会，邀请目标用户参与体验，与当地政府、行业协会等合作，扩大系统影响力。预计每两月一次，预计开展 6 次专项推广活动。

（2）专项培训，针对不同业务部室、公文写作需求、问答场景等，提供不同专题和程度的培训，预计每月 1 次，预计开展 12 次培训。

开展 6 次宣传与推广活动、制作宣贯和培训材料至少 4 次，开展专项培训 12 次。本阶段工作预计投入 2 人月，费用约 3 万。

5.1.3.4. 应用定期优化

（1）系统运行监控与维护，对大模型系统的运行状态进行实时监控，确保系统的高可用性和稳定性。故障响应与修复：建立快速响应机制，及时处理系统运行中的故障，包括应用级启停、系统级启停、功能响应失败等。

（2）功能优化与升级，根据用户反馈和实际使用情况，对公文写作大模型的功能进行优化，如提升文本纠错、智能问答的准确性和效率。

版本升级：定期更新系统版本，修复已知问题，引入新功能和性能改进。集成性优化，优化系统与其他业务系统的集成，如 OA 系统，确保数据交互的高效性和准确性。

（3）安全管理与应急响应，安全审计，定期进行系统安全审计，确保符合国家和行业安全标准。制定并执行应急响应计划，应对突发的安全事件或系统故障。

本阶段工作预计投入 6 人月，费用约 9 万。

5.2. 数据处理运营服务

构建标准化数据治理、语料库运营体系，保障政务数据时效性、安全性、合规性，支撑智能应用精准化服务。

5.2.1. 数据治理服务

5.2.1.1. 数据清洗

根据政务公文业务需求和数据特点，确定数据清洗的规则，对公文的数据缺失值和数据格式进行矫正。开展 4 次数据检查和清洗工作，每季度开展一次。

本阶段工作预计投入 8 人月，费用约 12 万。

5.2.1.2. 数据去重

（1）制定去重策略与标准：依据数据类型和特点，制定差异化去重策略。对于半结构化或非结构化数据，如公文文档、政策文件，采用 MD5 值、关键词提取等方法，计算数据相似度来识别重复内容。

（2）去重实施：实施数据去重的全流程，包括数据提取、去重处理、结果存储与验证。在数据提取阶段，根据去重范围和优先级，从不同数据源高效抽取数据；去重处理环节，运用选定的技术和策略对数据进行比对和筛选；处理后的结果存储至独立区域，便于后续验证和使用；最后，通过抽样检查、数据完整性校验等方式验证去重效果。

制定去重策略与标准，每月实施数据去重 1 次，共计 12 次。

本阶段工作预计投入 4 人月，费用约 6 万。

5.2.1.3. 非结构化数据转换

（1）数据分类与评估：全面梳理业务场景中的各类非结构化数据，详细分析不同数据类型并按照公文类型及业务场景分类。评估每种类型数据的规模、复杂性、潜在价值及应用场景，为后续制定针对性的转换策略提供依据。

（2）元数据提取：运用自然语言处理（NLP）技术，对文本内容进行分析。通过分词、词性标注和命名实体识别，提取部门、发文时间、发文编号等实体作为元数据。利用主题模型分析文本主题，提取 2-3 个主要主题作为元数据，帮助用户快速了解文本核心内容。同时，计算文本的关键词，选取出现频率较高且具有代表性的词汇作为元数据，便于文本检索和语义理解。

本阶段工作预计投入 6 人月，费用约 9 万。

5.2.2. 公共政务语料库更新与维护

根据业务需求建立数据更新机制：定期对数据资源池中的数据进行更新。及时将新出台的法律法规政策、最新的领导批示以及新增的公文数据等纳入数据资源池，保证数据的时效性和准确性。在数据更新过程中，进行数据质量检测，确保新加入的数据符合质量标准。

外部数据整合：关注政府公开数据平台、行业权威数据库、专业资讯网站等外部数据源。通过申请数据接口、下载数据包等方式获取外部数据。在采集过程中，严格遵守相关法律法规和平台使用规则，确保数据获取合法合规。

同时，对历史数据进行定期清理和优化，删除无用或过期数据，提高数据存储和处理效率。

本阶段工作预计投入 7 人月，费用约 10.5 万。

5.2.3. 私有政务语料库更新与维护

根据业务需求建立数据更新机制：定期对数据资源池中的数据进行更新。

每月更新一次语料库，添加新数据和修正旧数据，根据用户反馈，优化数据内容和结构，为智能审校、智能问答、智能写作等功能提供数据支持，并挖掘公文数据的潜在价值，支持决策和管理。

本阶段工作预计投入 4 人月，费用约 6 万。

5.2.4. 敏感词库更新与维护

（1）敏感词收集：组建专业团队负责敏感词库的日常维护，建立敏感词收集渠道，一方面密切关注国家法律法规、政策文件的更新，从中梳理可能涉及的敏感词汇；另一方面，收集日常公文处理、信息发布过程中发现的敏感词汇，以及相关部门通报的敏感信息。

（2）按照词汇的敏感程度、适用场景等进行分类管理及配置，如分为政治敏感词、安全敏感词、保密敏感词等，方便后续在公文处理和信息检索等环节精准匹配和管控。

（3）根据平台的使用反馈和实际业务需求变化，定期对敏感词库进行优化。对于一些不再具有敏感性或很少使用的词汇，进行清理；对于新出现的敏感概念或词汇，及时补充到词库中。

（4）提供定制化敏感词库服务，针对特定行业或场景的特殊需求，设计专属敏感词库，确保敏感信息管控的针对性和有效性。这包括但不限于金融行业、政务行业、新技术领域等，根据不同行业的规范和标准，定制相应的敏感词库，以满足客户的个

性化需求。

（5）为确保敏感词库的准确性和权威性，我们将定期对敏感词库进行审核和更新，及时调整和优化词库内容，确保敏感信息管控的合规性和有效性。同时，我们也将建立敏感词库的备份和恢复机制，以防止数据丢失或损坏，保障服务的连续性和稳定性。

本阶段工作预计投入 4 人月，费用约 6 万。

5.2.5. 驻场运维运营服务

项目执行支持：协助客户开展项目的具体执行工作，包括但不限于任务分配、进度跟踪、资源协调等，确保项目按计划推进。

技术咨询与解决：运用专业技术知识，为客户提供实时的技术咨询服务。针对项目执行过程中遇到的技术难题，迅速组织分析并制定解决方案，保障业务的连续性。

日常沟通与协作：作为客户团队的紧密合作伙伴，与客户内部各部门保持高效沟通，及时反馈工作进展及问题，积极参与团队协作，共同推动业务目标的实现。

派驻 1 名工程师，提供驻场服务，费用约为 23 万。

第六章 第三方服务

6.1. 监理服务

为保证项目能够顺利的开展，在横琴粤澳深度合作区行政事务局公文辅助 AI 系统建设（2025 年）项目实施期间须采购监理服务，监理方主要以“质量第一，预防为主，用科学、规范、诚信”作为监理原则，安排工作人员现场办公做好工程和项目进度和质量控制管理，协助单位完成工程任务并提供管理和技术咨询。项目要求以现场监理为主要监理方式，监理公司应派总监理工程师和监理工程师按采购人要求驻场，负责整个工程的全程监理工作。监理服务的主要内容包括：

总体把控：对项目的组织和实施计划安排、质量保证计划、进度控制计划等进行；

质量控制：依据合同要求和有关技术标准，审查、监督、控制本工程设备采购及设备安装的质量；

进度控制：审核承建单位的进度分解计划，确认分解计划可以保证总体计划目标，监督检查项目进度执行情况；

投资控制：通过对项目实施方案的优化，确保投资控制在合理、性价比高的范围内；

合同管理：对合同工期的延误和延期进行解释，协助业主处理项目实施的每个过程出现的合同变更、违约、索赔、延期、分包、纠纷调解及仲裁等问题；

信息管理：建立全面、准确反映项目各阶段工程状况的图表、文档，收集、管理项目各类文档和资料；

会议制度：为保证监理工作的开展和实施协调，监理方需组织必要的会议；

组织协调：建立畅通的沟通平台和沟通渠道，采取有效措施使项目信息在有关各方之间保持顺畅流通，积极协调项目各方之间的关系，推动项目实施过程中问题的解决。

监理服务的主要交付成果包括监理规划和实施细则、监理意见、监理通知单、监理总结报告等。

监理服务由横琴粤澳深度合作区行政事务局另行采购，不包含在本项目采购范围

内。

6.1.1. 监理服务目标

在项目咨询设计、决策支撑、规范化管理、需求方案的编制、需求方案评估、专家库管理、质量保证、进度推进等方面引入独立的第三方监理机构，协助采购人和用户方开展工作，提升项目实施质量与管理水平。

完成项目建设实施的监理目标，对本项目进行目标动态控制，实现建设单位在项目合同中确定的质量目标。

6.1.2. 监理服务内容

1．整体要求如下：坚持以“质量第一、预防为主、一切用数据说话，科学、公正、守法”作为监理原则，以“一协调：组织协调；二管理：合同管理、信息管理；三控制：投资控制、进度控制、质量控制”作为指导思想，协助采购人统筹管理、协调相关工程任务。

2．依据招标文件、投标文件、服务协议书，对服务在实施、交付、运行、验收阶段的服务质量进行审查、监督、及时向采购人及其指定的用户部门反映服务动态和监理工作情况；定期公布服务实施过程中的质量、进度、成本等有关数据指标，就项目中存在或出现的问题向采购人及其指定的用户部门提出第三方独立、公正、公平的意见建议或解决方案。

3．监督各方履行职责，协调各方的工作关系，建立畅通的沟通平台和沟通渠道，采取有效措施使项目信息在有关各方之间保持顺畅流通，积极协调项目各方之间的关系，推动相关问题的解决；检查督促服务提供商建立、完善安全生产制度，组织工程安全事故的调查与处理，确立财政投资信息化项目安全监督的工作目标。

6.1.3. 服务实施过程监理

服务实施阶段

（1）了解服务实施的环境条件准备情况。审核审核项目实施方案、计划的合法性、合理性，与设计方案的符合性。组织服务项目启动会；审批开工申请，确定开工日期，签发开工令；

（2）编制监理规划和实施细则；

（3）对服务实施相关的工程材料、硬件设备、系统软件的供货数量、质量检验。对服务实施各阶段的交付物质量进行检查，协助采购人及其指定的用户部门组织召开实施成果物评审会议；

（4）服务变更的风险评估和审核；

（5）监督服务实施进度计划的执行，发现实施进度偏离时，要求服务供应商调整或修改计划，采取必要措施加快采购进度，以使实际施工进度符合合同的要求；

（6）组织召开项目例会、专项会议，定期向采购人及其指定的用户部门汇报服务实施进展情况。组织信息系统项目质量、系统集成质量事故的原因调查、问题分析、问题评估、事故处理；监控软件开发过程质量。监督需求管理、配置管理的执行和控制情况，督促承建商整改存在的问题。对承建商提供设备性能指标及产品厂家供货证明函等进行严格审核。对承建商负责采购的设备、材料按合同规定的标准进行检验验收；

（7）审查所监理的信息化项目进度计划，并监督计划的执行。确定项目实施工作的顺序，控制项目实施的进度。发现信息系统项目未能按计划进行时，要求承建商调整或修改计划，采取必要措施加快开发进度，以使实际项目进度符合合同的要求。协助采购人管理项目合同，监督检查承建商履行合同，协助采购人检查所监理的信息化项目实施过程出现的违约、索赔、延期、分包、纠纷调解及仲裁等问题；

（8）及时向采购人提交反映所监理的信息化项目动态信息和监理工作情况的项目文档。建立全面、准确反映各自项目的软件开发各阶段状况的图表、文档，收集、管理项目各类文档和资料。督促、检查承建商及时完成各阶段设计文档、代码、会议纪要、变更单、问题跟踪单等资料的整理和归档工作。审查承建商的设计文档、变更单、问题跟踪单，审查承建商与采购人之间的业务联系单、备忘录、电子邮件、传真、电话记录等，并加具意见；

（9）协助采购人划分或澄清承建商的工作范围和职责。监督承建商履行职责，协调各方的工作关系。建立畅通的沟通平台和沟通渠道，采取有效措施使项目信息在有关各方之间保持顺畅流通，积极协调项目各方之间的关系，推动项目实施过程中问

题的解决。督促承建商建立完善的信息安全管理制度，数据备份制度。组织信息安全事故的调查与处理。建立监理的信息安全管理工作目标和管理流程。提高项目整体的信息安全水平。

（10）督促检查承建商及时完成各阶段设计文档、测试记录、变更记录、问题跟踪处理记录等文件的归档工作，按归档要求进行分类整理归档，按时完成竣工资料（包括监理工作方面的归档资料）验收。确保信息系统项目中各类文件传送的规范化、制度化，监理类文书资料管理的科学化、规范化。监理方的文档管理人员，负责收集、管理监理工作各类文书资料，对监理工作文档、收发文签收登记等进行管理；

（11）其他监理工作。

6.1.4. 服务交付阶段

（1）审查服务提供商提交的服务交付申请；

（2）协助组织服务项目第三方测评，监督服务提供商对测评问题的整改；

（3）协助组织服务交付验收评审，出具服务交付验收报告；

（4）督促、检查服务提供商对服务项目培训情况与成效；

（5）记录服务项目遗留问题（如存在），并跟踪解决；

（6）参与系统功能的测试、集成、竣工验收和交接；

（7）其他监理工作。

6.1.5. 服务运行过程监理

服务运行阶段

（1）审核服务提供商提交的服务项目运行总体方案；

（2） 监查服务运行情况，记录相关运行数据；

（3）记录服务运行期间出现的质量问题，并责成服务提供商解决，跟踪解决情况；

（4）监督服务运行期间，服务提供商的服务质量包括故障处理、服务响应、用户评价等，出具监理评价报告。

（5）跟踪所监理的信息化项目在质保期内的运行状况，督促承建商做好售后服

务；

（6）其他监理工作。

6.1.6. 服务验收阶段

（1）审核服务提供商提交的服务运行总结报告，确认服务项目是否达到最终验收要求；

（2）协助采购人及其指定的用户部门、服务提供商筹备、审查服务项目档案；

（3） 审查服务有关的设备、材料、软件、文档等移交；

（4）编制和提交服务验收监理报告，向采购人提交最终监理档案资料；

（5） 协助采购人及其指定的用户部门组织开展服务验收；

（6）签署最终服务验收报告；

（7）审核服务提供商提交的服务结算文档，审查结算金额；

（8）其他监理工作。

6.1.7. 监理服务组织管理

监理服务组织管理

人员类别	数量	具体要求
总监理工程师	1 名	负责总体负责本项目的技术指导，对项目重大技术问题进行决策。具有硕士或以上学位，信息系统监理师证书，具有 10 年或以上信息工程监理项目经验，良好的项目管理和团队领导能力。
总监理工程师代表	1 名	负责项目的日常技术指导和监理团队统筹管理，负责项目全流程监理工作。具有大学本科或以上学位，信息系统监理师证书，具有 5 年或以上信息工程监理项目经验，良好的项目管理和团队领导能力。

项目助理	1 名	配合项目经理完成工作，负责做好监理任务接收、监理合同签订、监理文档管理、内部沟通协调等，支撑监理团队。
监理工程师	1 名	监理工程师团队，负责保证监理的信息系统项目能够按时、按质、按量实施和竣工。具备监理工程师相应证书。

6.1.8. 范围、进度、质量、风险控制措施

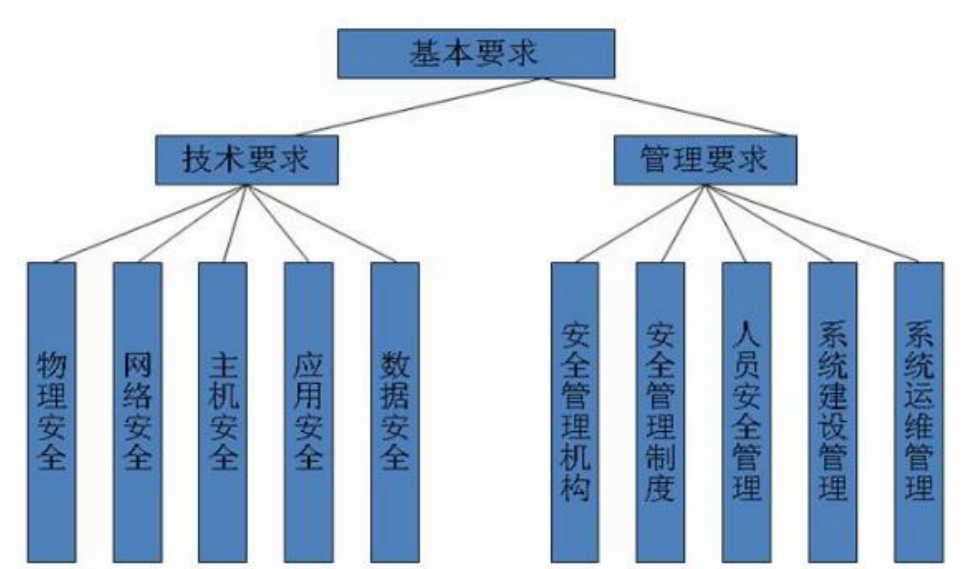
监理方在项目实施过程中，需对项目进行规范化管理，要有项目实施组织、项目实施管理计划、项目进度计划、项目验收计划等方案，确保项目质量。

监理方应成立相应的项目组，并指定专职的项目责任人负责项目协调和调度工作。项目责任人在项目实施过程中不得更换。其他人员原则上不得更换，若确需更换，须书面向招标人提出申请，并获得招标人认可。更换人员个人资质不低于原项目组人员。

6.2. 网络安全等级保护测评服务

6.2.1. 业务信息安全等级保护

等级保护工作作为我国信息安全保障工作中的一项基本制度，对提高基础网络和重要信息系统安全防护水平有着重要作用，在《信息系统安全等级保护基本要求》中对信息安全管理和信息安全技术也提出了要求，如下图所示。



本次横琴粤澳深度合作区行政事务局公文辅助 AI 系统项目对业务信息安全被破坏时所侵害的客体主要有公民、法人和其他组织的合法权益和社会秩序、公共利益，侵害程度最多为一般损害。

根据公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定的《信息安全等级保护管理办法》、《信息系统安全等级保护定级指南》等标准，本项目参照信息安全等级保护三级进行建设。

本项目将综合考虑各方面安全因素，严格遵循国家信息安全等级保护建设、测评、整改和维护的相关要求，遵循安全开发规范和安全制度，利用目前比较先进的应用集成技术，实现身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、保密性、抗抵赖、软件容错、资源控制和代码安全管理等方面的应用安全。

1．物理安全

基于物理位置、访问控制、防盗、防破坏、防雷击、防火、防水、防潮、防静电、温湿度控制、电力供应以及电磁防护的整体安全防护要求，实现全面的物理安全。

2．网络安全

基于网络结构、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范和网络设备防护的具体内容进行整体安全防护。

3．主机安全

基于身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范

和资源控制的具体内容进行整体安全防护。

4．应用安全

基于应用身份鉴别、访问控制、安全审计、通信完整性、保密性、抗抵赖、剩余信息保护、软件容错和资源控制的具体内容进行整体安全防护。

5．数据安全和备份恢复

基于数据完整性、保密性以及备份和恢复的具体内容进行整体安全防护。

6.具体安全措施

RBAC 基于角色的访问权限控制；基于用户的数据权限过滤密码等关键数据传输加密；用户只能同时登陆一个客户端。

7. 业务信息描述

横琴粤澳深度合作区行政事务局中间业务信息包括：企业信息和人员信息。属于公共、法人和其他组织的专有信息。

业务信息受到破坏时所侵害客体的确定（侵害的客体包括：1 国家安全，2 社会秩序和公共利益，3 公民、法人和其他组织的合法权益等共三个客体）该业务信息遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益。侵害的客观方面（客观方面是指定级对象的具体侵害行为，侵害形式以及对客体的造成的侵害结果）表现为：一旦信息系统的业务信息遭到入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对公民、法人和其他组织的合法权益造成影响和损害，可以表现为：影响正常工作的开展，导致业务能力下降，造成不良影响，引起法律纠纷等。

信息受到破坏后对侵害客体的侵害程度（即上述分析的结果的表现程度）。

上述结果的程度表现为严重损害，即工作职能受到严重影响，业务能力显著下降，出现较严重的法律问题，较大范围的不良影响等。

6.2.2. 确定业务信息安全等级

查《中华人民共和国国家标准 GB17859-1999---信息系统安全等级保护定级指南》表可知（以后简称《定级指南》），业务信息安全保护等级为第三级。

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

6.3. 商用密码应用建设方案编制及安全性评估服务

参照《广东省省级政务信息化项目商用密码应用工作指引》（2022 年修订版）（粤密码协调组〔2022〕6 号，以下简称《工作指引》）文件要求执行。

①商用密码应用建设方案编制服务

按照《工作指引》附件 2 和附件 4，编制商用密码应用建设方案。

②商用密码应用安全性评估服务

根据《工作指引》文件要求组织专家或委托密评机构对商用密码应用建设方案进行评估，出具《商用密码应用方案评估报告》。

完成项目建设后，委托密评机构进行商用密码应用安全性评估，并出具《商用密码应用安全性评估报告》。

本项目中，参照《广东省省级政务信息化项目商用密码应用工作指引》（2022 年修订版）（粤密码协调组〔2022〕6 号，以下简称《工作指引》）文件要求执行。建设单位的政务云平台密码保障系统，采用符合国家密码管理部门要求的密码技术来保护云平台及数据的安全性，包括但不限于网络和通信安全、设备和计算安全、应用和数据安全、密钥管理等。

同时，建设单位建立了完善的密钥管理机制，采用技术和管理措施，从密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等全流程各环节，保障密钥安全。

针对云间的安全性，建设范围规划的政务云平台采取数据安全分级和加密、建设

专线等方式来保障其安全性，包括根据数据重要性和敏感程度，进行数据分级传输和加密，实现过程控制和双向安全防护；通过数据共享平台实现云间数据同步、断点重传、数据迁移、数据加密等功能，保证传输过程中的真实性和可靠性；在多云节点间建设专用线路或者 VPN 专网，实现传输链路的独占性，防止数据被监听、复制、篡改和植入。

6.3.1. 密码应用现状

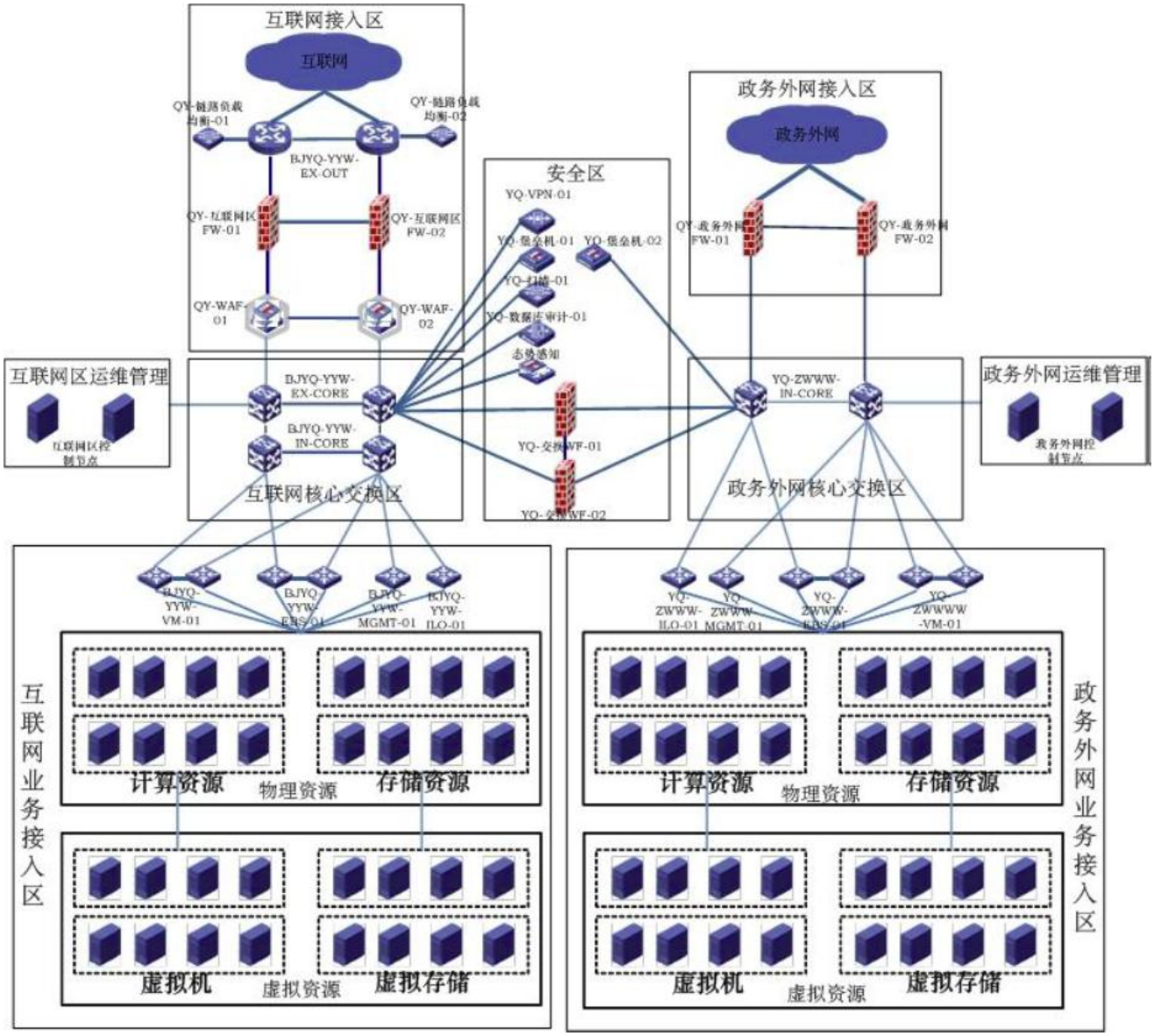
6.3.1.1. 基本情况

本项目系统部署在云机房，部署有互联网区和政务外网区，及安全区域（含数据交换区）和运维管理区域，主要服务于政务云运维人员和管理人员。用户通过 SSL VPN 单点拨入后访问云管理平台资源。

本项目计划利旧横琴粤澳深度合作区现有密码资源池提供密码服务，密码应用符合以下信息安全合规性和密码应用的要求，已按照密码应用安全性评估管理办法和相关标准，通过密码应用的安全性测评。

平台每年定期进行网络安全等级保护定级备案（测评机构：市信息安全测评中心），定级等级为第 3 级（S3A3G3）。同时已通过国家网信办“云计算服务安全评估”。

6.3.1.2. 系统网络拓扑



政务云平台，由云平台软件、服务器设备、网络交换机设备、安全审计设备、安全防御设备以及机房基础设施构成，按照信息系统安全等级保护三级标准进行建设。整个平台分为政务外网资源区（简称：政务外网区）及政务互联网资源区（简称：互联网区）。

6.3.1.3. 系统软硬件构成

系统部署有服务器、磁盘阵列、堡垒机、防火墙等硬件设备，机房门禁系统对进

出机房人员进行身份鉴别，使用视频监控系统对机房视频监控数据进行管理，计算机终端通过浏览器访问登录运维系统。

6.3.2. 关键应用列表

序号	应用名称	主要功能
1	人工智能辅助办公系统	公文辅助 AI 系统底座建设：构建基于大数据、人工智能技术的公文辅助 AI 系统底座，为平台提供强大的数据支撑和计算能力。

6.3.3. 密码应用需求分析

6.3.3.1. 密码应用合规性需求分析

本项目计划利旧现有密码资源池提供密码服务，密码应用符合以下信息安全合规性和密码应用的要求，已按照密码应用安全性评估管理办法和相关标准，通过密码应用的安全性测评。

密码应用相关要求

（1）宜采用密码技术进行物理访问身份鉴别,保证重要区域进入人员身份的真实性；

（2）宜采用密码技术保证电子门禁系统进出记录数据的存储完整性；

（3）宜采用密码技术保证视频监控音像记录数据的存储完整性；

（4）以上如采用密码服务,该密码服务应符合法律法规的相关要求,需依法接受检测认证的,应经商用密码认证机构认证合格；

（5）以上采用的密码产品,应达到 GB/T37092 二级及以上安全要求。

6.3.3.2. 网络和通信安全

1.密码应用相关要求

（1）应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；

（2）宜采用密码技术保证通信过程中数据的完整性；

（3）应采用密码技术保证通信过程中重要数据的机密性；

（4）宜采用密码技术保证网络边界访问控制信息的完整性；

（5）可采用密码技术对从外部连接到内部网络的设备进行接入认证,确保接入的设备身份真实性；

（6）以上如采用密码服务,该密码服务应符合法律法规的相关要求,需依法接受检测认证的,应经商用密码认证机构认证合格；

（7）以上采用的密码产品,应达到 GB/T 37092 二级及以上安全要求。

2.风险分析

（1）目前管理人员通过 SSL VPN 单点拨入后访问平台资源，VPN 采取用户名/口令登录+手机验证码两种组合并以 HTTPS 方式访问云管理平台进行登录和身份鉴别，其中 HTTPS 加密协议采用算法为 RSA，为弱算法，存在高风险，未使用合规的密码技术对通信双方进行验证，存在非法设备从外部接入内部网络，通信数据在信息系统外部被非授权截取、非授权篡改风险。

（2）目前管理人员通过连接 VPN 登录到堡垒机采取 SSH 对系统中的服务器、存储等设备进行远程管理，未使用合规的密码协议建立安全管理通道，存在搭建的集中管理通道被非授权使用，或传输的管理数据被非授权获取和非授权篡改风险。

6.3.3.3. 密码应用需求

（1）使用符合密码相关国家、行业标准要求的 SSL VPN 安全网关，通过 VPN 拨入后 PC 端浏览器访问云管理平台时，实现对通信实体的身份鉴别，建立安全的数据传输通道。

（2）使用符合密码相关国家、行业标准要求的 SSL VPN 安全网关，使用 SSL VPN 登录到堡垒机建立安全的集中管理通道。

（3）使用符合密码相关国家、行业标准要求的 SSL VPN 安全网关，对网络边界访问控制信息进行完整性保护。

6.3.3.4. 设备和计算安全

1.密码应用相关要求

（1）应采用密码技术对登录设备的用户进行身份鉴别.保证用户身份的真实性；

（2）远程管理设备时,应采用密码技术建立安全的信息传输通道；

（3）宜采用密码技术保证系统资源访问控制信息的完整性；

（4）宜采用密码技术保证设备中的重要信息资源安全标记的完整性；

（5）宜采用密码技术保证日志记录的完整性；

（6）宜采用密码技术对重要可执行程序进行完整性保护,并对其来源进行真实性验证；

（7）以上如采用密码服务,该密码服务应符合法律法规的相关要求,需依法接受检测认证的，应经商用密码认证机构认证合格；

（8）以上采用的密码产品,应达到 GB/T 37092 二级及以上安全要求。

2.风险分析

（1）目前系统运维管理人员通过使用 VPN 登录到堡垒机，登录堡垒机采用用户名/口令+短信验证码方式进行身份鉴别，未使用合规的密码产品对管理员登录进行身份鉴别，未使用合规的密码技术建立安全的远程管理传输通道，存在设备被非授权人员登录、身份鉴别数据被非授权获取或非授权使用等风险。

（2）目前云管理平台服务器设备日志均明文存储，未使用密码技术进行完整性保护，存在设备日志记录被非授权篡改风险。

6.3.3.5. 应用和数据安全

1.密码应用相关要求

（1）应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；

（2）宜采用密码技术保证信息系统应用的访问控制信息的完整性；

（3）宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；

（4）应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；

（5）应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；

（6）宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；

（7）宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；

（8）在可能涉及法律责任认定的应用中,宜采用密码技术提供数据原发证据和数据接收证据,实现数据原发行为的不可否认性和数据接收行为的不可否认性；

（9）以上如采用密码服务,该密码服务应符合法律法规的相关要求,需依法接受检测认证的,应经商用密码认证机构认证合格；

（10）以上采用的密码产品,应达到 GB/T 37092 二级及以上安全要求。

2.风险分析

（1）系统管理人员通过 SSL VPN 单点拨入后，以 IP 方式访问云管理平台采用用户名/口令+手机验证码两种组合进行登录和身份鉴别，未使用合规的密码技术对登录用户进行身份鉴别，存在云管理平台被非授权人员登录风险。

（2）云管理平台对用户权限根据用户策略进行访问控制，未使用密码技术对用户访问权限控制列表进行完整性保护，存在应用资源被非授权用户获取的风险。

（3）目前云管理平台中的用户身份信息数据和业务信息数据在系统中存储，未使用密码技术进行传存储机密性、完整性保护，存在身份鉴别等数据被窃取和非授权篡改风险。

（4）目前云管理平台中的日志数据存储在应用服务器中，未使用密码技术进行完整性保护，存在应用日志记录被非授权篡改风险。

6.3.3.6. 云平台自身密码应用需求

1.身份鉴别需求

对访问云资源的云平台管理员、用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒、防重用，保证云平台管理员身份的真实性。以及云平台管理员和用户的关键操作不可否认性需求。

2.敏感信息的安全存储需求

保证快照文件、租户镜像、身份鉴别信息、重要业务数据、密钥、云资源管理信息、审计日志等敏感信息在存储过程中的保密性和完整性。

3.敏感信息的传输需求

保证身份鉴别信息、云资源管理信息、重要业务数据、密钥等敏感信息在传输过程中的保密性和完整性。

4.虚拟机迁移安全需求

虚拟机监控器之间用来发起和管理虚拟机动态迁移的通信机制应该加入身份鉴

别和防篡改机制，以保证虚拟机在迁移过程中的控制平面安全，对虚拟机迁移的数据通信信道必须进行安全加固，以保证虚拟机在迁移过程中的数据平面安全，防止被动攻击（如监听）和主动攻击（如篡改）。

5.关键操作不可否认性需求

需要对云平台管理员的关键操作进行不可否认性的保护。

6.3.3.7. 云上应用系统密码应用需求

1.身份鉴别需求

对访问云上应用系统的用户和系统管理员进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证云上应用系统的用户和系统管理员身份的真实性。

2.云上数据安全存储需求

云上应用系统的数据库中，存在明文存储敏感业务数据的情况，开发人员、业务人员、运维人员都可能直接接触到数据本身，需要通过密码技术实现密文存取、操作和访问，保证存储数据的机密性。

3.完整性保护安全需求

云上应用系统的访问控制信息、日志记录需使用密码技术实现完整性和不可否认性的保护。

4.数据安全传输需求

云上应用系统的身份鉴别信息、重要业务数据、密钥等重要数据在传输过程中进行机密性、完整性保护。

6.3.4. 关键数据列表

序号	关键数据	关键数据描述	安全需求
1	用户身份数据	人工智能辅助办公系统用户身份鉴别数据	保密性、完整性
2	账号权限数据	人工智能辅助办公系统用户账号权限鉴别数据	保密性、完整性
3	日志数据	人工智能辅助办公系统管理员操作日志、云管理平台运行日志	完整性
4	公文数据	人工智能辅助办公系统接收和发送的公文原文件，以及经标注后的可被模型读取的公文	保密性、完整性

		数据	
5	模型服务数据统计	人工智能辅助用户在办公场景使用效果数据。	完整性

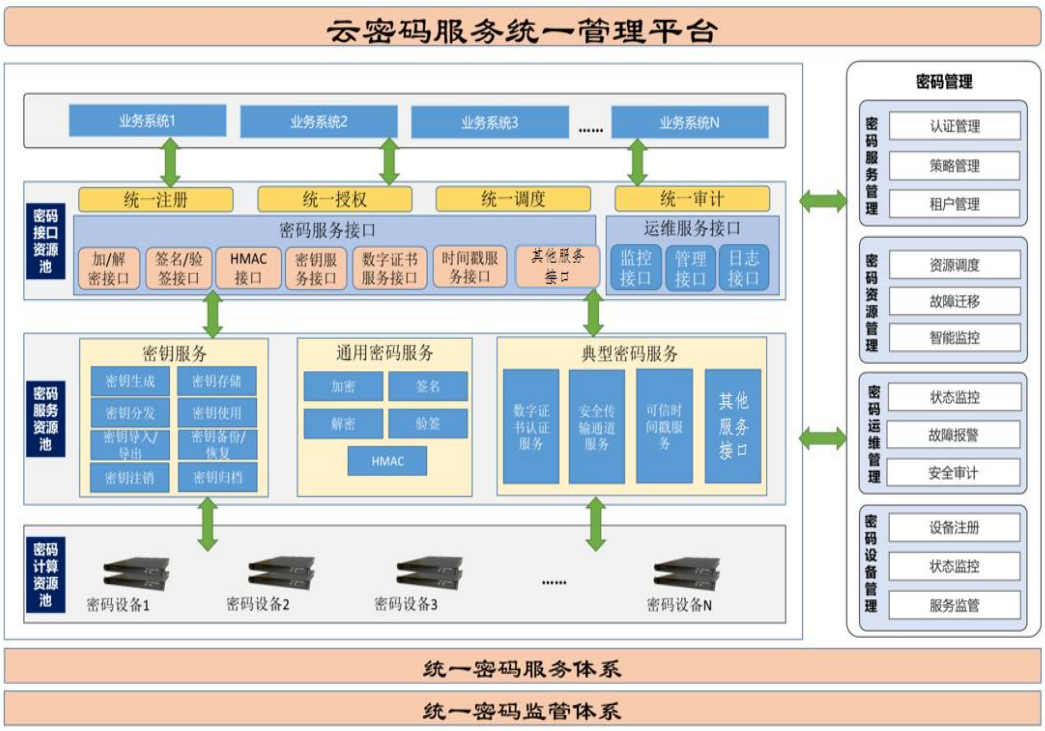
6.3.5. 密码应用技术方案

6.3.5.1. 总体设计思路

通过建设集约化的密码基础设施为云提供一体化、虚拟化、可视化的密码应用综合服务，密码基础设施包括可视化云密码统一服务平台、云服务器密码机、签名验签与时间戳二合一服务器、数字证书认证系统、智能密码钥匙等密码软硬件设备，这些密码基础设施通过定制化和标准化两类密码服务接口，为云平台自身和云上应用提供一站式的云密码应用支撑服务。

6.3.5.2. 密码应用技术框架

云密码应用技术框架如下图所示。根据云的部署方式和实现业务功能，在满足安全性、稳定性、可管理性原则的基础上，在云平台通过部署云服务器密码机、数字证书认证系统、签名验签与时间戳二合一服务器、可视化云密码统一服务平台等密码产品，并正确部署配置，以满足云的密码应用需求。



图：云密码应用技术框架

密码计算资源池由云服务器密码机、签名验签与时间戳二合一服务器等密码硬件设备和数字证书认证系统、可视化云密码统一服务平台等密码软件系统组成，为上层密码服务资源池提供基础密码计算服务、密钥管理服务、数字证书管理服务等密码支撑服务。

云平台及云上应用系统所的密码服务通过统一标准的密码服务接口调用方式实现，以满足身份鉴别、授权管理、访问控制、数据安全防护等方面的密码应用需求。

密码管理主要依托可视化云密码统一服务平台实现，在平台上可查看到各类密码软硬件设备的运行情况。

6.3.5.3. 网络和通信安全设计

按照 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》第三级信息系统网络和通信安全的基本要求，对云网络和通信安全进行设计。

应用于网络和通信安全的密码应用的措施如下：

1)用户在访问云管系统前，用户先通过部署在网络边界的 VPN 设备基于数字证书

对通信双方进行身份鉴别，通过信息加密传输防止通信数据被非法截获、假冒和重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性；

2)通过在网络边界部署 VPN 设备，保证网络边界和系统资源访问控制信息的完整性；

3)通过在网络边界部署 VPN 设备，采用国密 SSL 技术保证传输过程中重要数据的完整性；

4)通过在网络边界部署 VPN 设备，采用加密技术保证传输过程中重要数据的机密性；

5)通过在网络边界部署 VPN 设备，基于国密 SSL 协议建立一条安全的信息传输通道，对云网络中的设备进行集中管理。

6.3.5.4. 设备和计算安全设计

按照 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》第三级信息系统设备和计算安全的基本要求，对云的设备和计算安全进行设计。

应用于设备和计算安全的密码应用的措施如下：

1) 通过 SSL VPN 网关，对登录云中设备的用户进行身份标识和身份鉴别，保证身份标识具有唯一性，防止假冒运维人员登录设备；

2) 设备管理员、运维人员在远程管理设备时，在客户端与 SSL VPN 网关间建立基于国密 SSL 协议的信息传输通道，并对设备管理员身份进行身份鉴别，保证远程管理时传输数据的机密性和完整性。

3) 在运维管理区部署日志服务器，将云中设备的日志发送至日志服务器中，日志服务器调用云服务器密码机虚拟出的虚拟密码机对采集的设备日志数据计算消息鉴别码，将设备日志数据与消息鉴别码一同存储在数据库中，实现云中设备日志数据的完整性保护。

6.3.5.5. 应用和数据安全设计

按照 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》第三级信息系统应用和数据安全的基本要求，对云的云管系统的应用和数据安全进行设计。

应用与数据安全密码应用的措施如下：

1) 使用 SSL VPN 对登录云管系统的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证访问云管系统的用户身份的真实性；

2) 在管理人员客户端和运维人员客户端上部署 VPN，使用 SSL VPN 对云管系统与管理人员客户端、运维人员客户端之间传输的重要数据进行加密，实现重要数据在传输过程中的机密性保护；

3) 使用 SSL VPN 对云管系统与管理人员客户端、运维人员客户端之间传输的重要数据基于国密 SSL 协议进行完整性保护，保证重要数据在传输过程中的完整性。

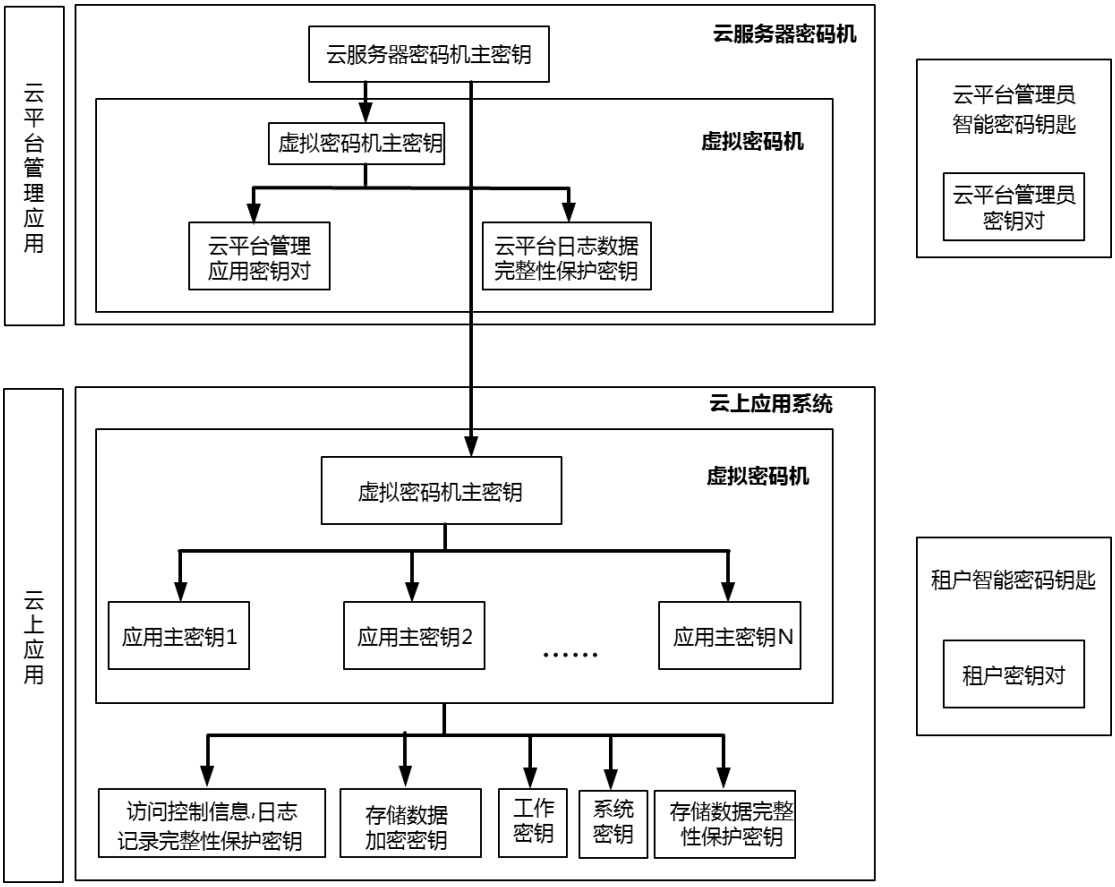
4) 部署符合密码相关国家、行业标准要求的云服务器密码机，在运维管理区部署日志服务器，云管系统将日志数据上传至日志服务器中，日志服务器通过调用云服务器密码机虚拟出的虚拟密码机对采集的云管系统日志数据计算消息鉴别码，将日志数据与消息鉴别码一同存储在数据库中，实现云管系统日志数据的完整性保护。

6.3.5.6. 密钥管理设计

6.3.5.6.1. 云平台密钥管理体系设计

云使用的密钥主要有云管系统用户的签名密钥、加密密钥，IPSEC/SSL VPN 安全网关设备密钥、云服务器密码机的设备密钥、签名验签与时间戳二合一服务器设备密钥。

云采用 PKI 技术对各个实体进行身份标识，由自建数字证书认证系统为云平台管理系统、云上应用系统、云平台管理员、云平台运维人员、租户和用户签发标识其身份的证书，其密钥对包括签名密钥对和加密密钥对。云平台管理系统、云上应用系统的证书（含私钥）保存在虚拟密码机中，云平台管理员、云平台运维人员和租户的证书（含私钥）保存在智能密码钥匙中。就云本身的密钥体系而言，可以分为云平台管理应用层和云上应用层两层密钥，如图所示。



图：云密钥体系图

1）云平台管理应用层

将云服务器密码机虚拟出虚拟密码机服务于云平台管理应用，通过云服务器密码机的主密钥，对以下两类密钥进行保护：

1、 云平台管理应用密钥对（签名密钥对、加密密钥对）：用于进行云平台管理应用和云平台管理员/租户之间的身份鉴别和密钥协商。

2、 虚拟密码机主密钥：在虚拟密码机创建并初始化时，由云服务器密码机机内置密码卡生成；用于对虚拟密码机的相关密钥进行保密性和完整性保护。

2）云上应用层

虚拟密码机服务于云上应用。租户可能有多个应用，共分三层密钥体系：虚拟机主密钥保护应用主密钥；而各个云上应用通过自己的应用主密钥对以下三类密钥进行保护：

1、云上应用的访问控制信息、日志记录保护密钥。对访问控制信息、日志记录进行完整性保护。

2、云上应用的存储数据加密密钥。对存储重要数据进行机密性保护。

3、云上应用的存储数据完整性保护密钥。对存储重要数据进行完整性保护。

4、云上应用的系统密钥对。用于云上应用和租户/用户之间的身份真实性鉴别和密钥协商。

5、云上应用的工作密钥。用于加密传输应用数据至用户端。

6.3.5.6.2. 云密钥生命周期管理

云服务器密码机主密钥	
密钥生成	设备初始化时，由设备内置密码卡生成。
密钥存储	安全存储在设备的内置密码卡的密钥存储区。
密钥分发	不涉及。
密钥导入与导出	不涉及。
密钥使用	用于保护虚拟密码机主密钥。
密钥备份与恢复	采用设备自身的密钥备份机制进行备份。
密钥归档	不涉及。
密钥销毁	设备再次初始化时，密钥被销毁。

虚拟密码机主密钥	
密钥生成	虚拟密码机初始化时，由云服务器密码机内置密码卡生成。
密钥存储	安全存储在云服务器密码机的内置密码卡的密钥存储区。
密钥分发	不涉及。
密钥导入与导出	不涉及。
密钥使用	用于保护虚拟密码机中的应用主密钥。
密钥备份与恢复	采用设备自身的密钥备份机制进行备份。
密钥归档	可由运维管理区的密钥管理系统进行密钥归档。
密钥销毁	虚拟密码机再次初始化时，密钥被销毁。

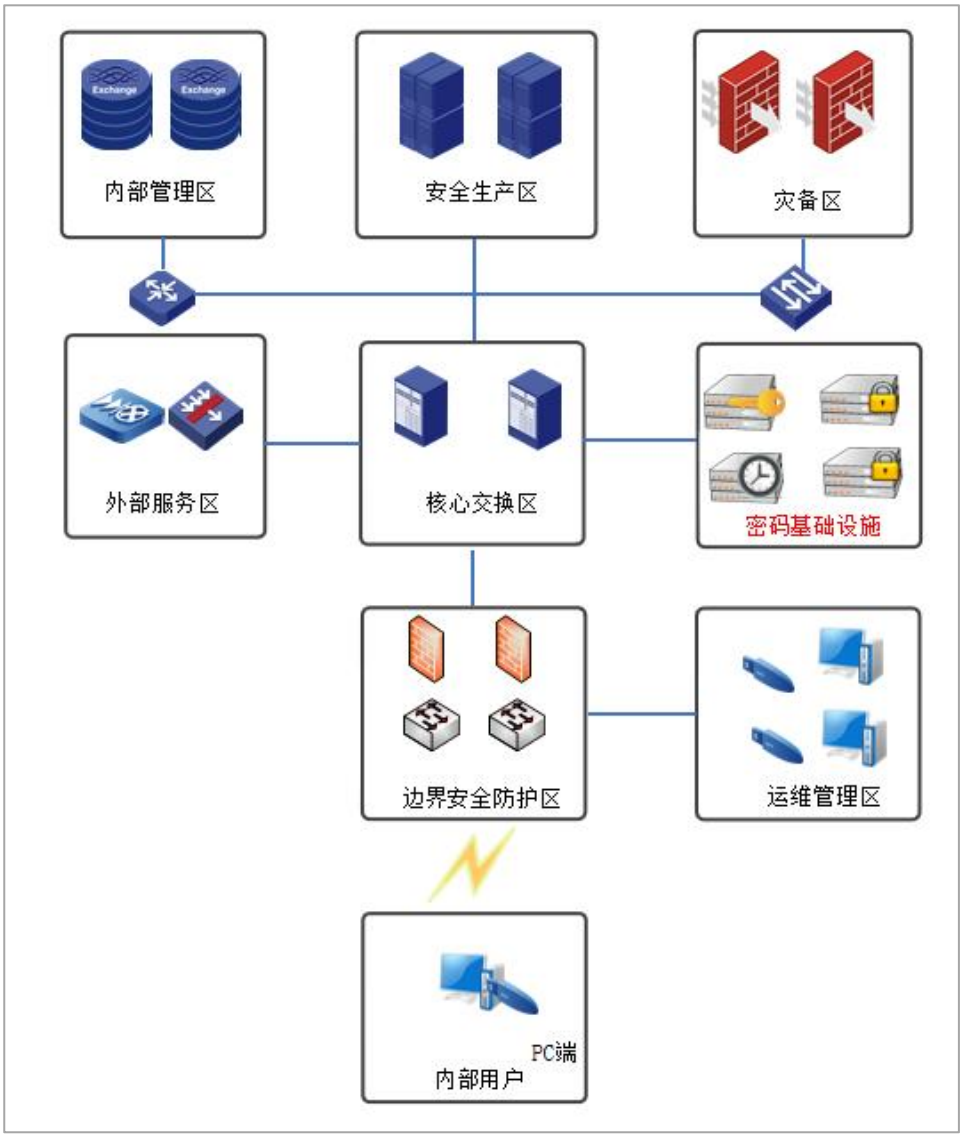
应用主密钥	
密钥生成	当云管系统将虚拟密码机分配给应用系统时，由虚拟密码机调用云服务器密码机内置密码卡生成。
密钥存储	安全存储在云服务器密码机的内置密码卡的密钥存储区。
密钥分发	不涉及。
密钥导入与导出	不涉及。
密钥使用	用于保护云上应用系统的访问控制信息、日志数据完整性保护密

	钥、存储数据加密密钥、存储数据完整性保护密钥。
密钥备份与恢复	采用设备自身的密钥备份机制进行备份。
密钥归档	可由运维管理区的密钥管理系统进行密钥归档。
密钥销毁	虚拟密码机再次初始化时，密钥被销毁。

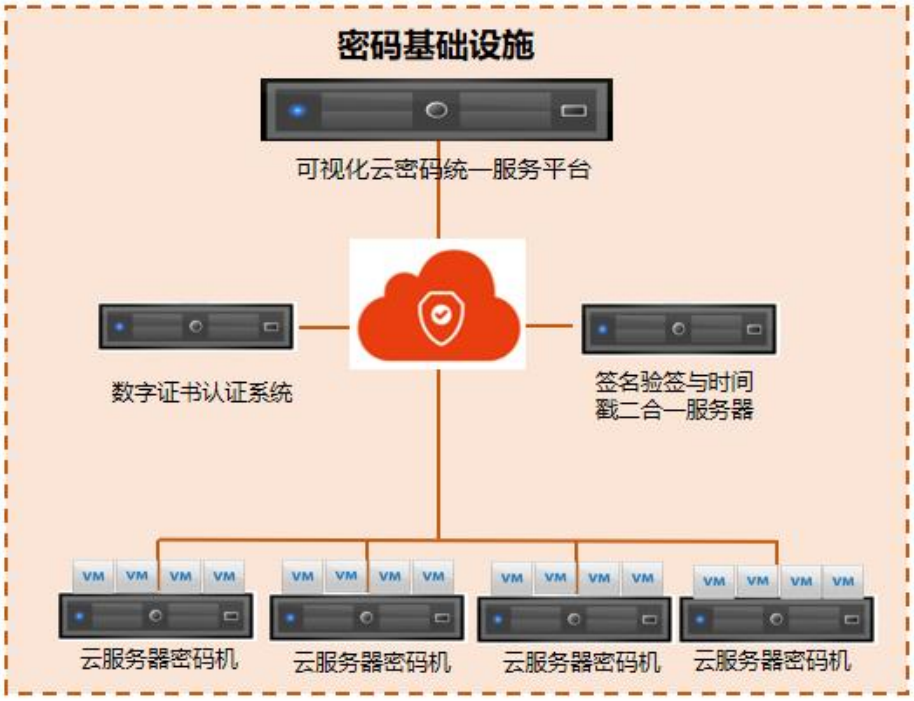
云平台日志数据完整性保护密钥（对称密钥）	
密钥生成	由虚拟密码机调用云服务器密码机内置密码卡生成。
密钥存储	安全存储在云服务器密码机的内置密码卡的密钥存储区。
密钥分发	不涉及。
密钥导入与导出	不涉及。
密钥使用	用于云管系统日志数据的完整性保护。
密钥备份与恢复	采用设备自身的密钥备份机制进行备份。
密钥归档	可由运维管理区的密钥管理系统进行密钥归档。
密钥销毁	虚拟密码机再次初始化时，密钥被销毁。

6.3.5.7. 密码应用部署

以下是云网络部署示意图和密码资源平台部署示意图：



图：云网络部署示意图



图：密码基础设施部署示意图

在运维管理区划分一个安全区域（密码服务区）用于部署密码基础设施，包括云服务器密码机，签名验签和时间戳二合一服务器、数字证书认证系统、可视化云密码统一服务平台，为云平台及云上应用提供加解密、签名验签、可信时间、数字证书签发、密码综合管控等服务；PC 终端用户配置智能密钥钥匙，提供身份鉴别、密钥安全存储、数字签名、本地数据机密性和完整性保护等服务。

（1）云服务器密码机：主要为云平台及云上应用系统提供数据加解密、签名验签、杂凑等密码运算服务，实现信息的机密性、完整性、真实性和不可否认性保护，同时配合运维管理区的密钥管理系统提供安全、完善的密钥管理功能。

（2）签名验签和时间戳二合一服务器：该设备集合了签名验签与 时间戳两类密码设备的功能，可以为用户及设备提供身份鉴别，为数据提供签名验签等功能，时间戳能够唯一地标识某一时刻（通常为一段字符序列），从而可用于云和云上应用系统日志数据的产生时间，确保日志数据基于时间的真实性及不可否认性。

（3）数字证书认证系统：主要为设备/用户等实体的身份鉴别提供真实性、身份验证、签名验签等信任服务。

（4）可视化云密码统一服务平台：对密码设备及密码服务进行统一纳管，集中为云提供数字证书签发、密钥管理、加解密、签名验签等各项密码服务。还可以对云上密码软硬件产品的运行状态进行监控，并以可视化的方式展示密码产品和密码服务的应用情况。

序号	产品名称	部署位置	功能简述	使用的密码算法	数量	用途
1	浏览器密码模块（二级）	互联网区/运维终端区	支持国密算法，支持方案国密应用服务站点，实现客户端到服务端的业务安全访问。	SM2/3/4	按需配置	运维人员/管理员安全登录系统
2	服务器密码机	安全管理区	支持密钥管理、密钥生成，可对接数字证书认证系统，提供密钥安全管理；支持国密算法。	SM2/3/4	1	为数字证书系统提供密码计算
3	高性能密码应用服务器	安全管理区	密码应用系统专用硬件设备，双电源 750W-850W，6 核 12 线程 CPU X2，2T 硬盘，128G 内存;L4：新建：1.45M CPS、并发：32M、吞吐：72Gbps；L7：新建：440KRPS、并发：4.8M、吞吐：50Gbps；支持数字证书认证系统	SM2/3/4	1	为数字证书认证系统和日志完整性保护系统提供基础平台
4	数字证书认证系统	安全管理区	数字证书认证系统由 RA、CA、KMC、OCSP、LDAP 等模块组成，提供数字证书申请、注册、签发等证书全生命周期管理，支持 SM2 算法。	SM2/3/4	1	为设备/用户的身份鉴别提供真实性服务
5	动态令牌认证系统	安全管理区	动态令牌认证系统由动态密码种子生成、验证服务和服务管理三个子系统组成，支持一次一密双因素认证，最大支持 200	SM2/3/4	1	供动态令牌调用，鉴别用户身份

			万用户，响应性能6000TPS,支持国密算法。			
6	SSL VPN 安全网关系统	安全管理区	SSL VPN 系统集成了安全认证、应用防火墙、N+1 Cluster、虚拟桌面接入、虚拟 VPN、CIFS/NFS 文件共享等功能,L3-L7 最大支持 72000 在线用户,最多支持 256 个虚拟门户。SSL 吞吐:4.5G,支持 SM2 算法。	SM2/3/4	1	为互联网运维人员提供安全接入通道
7	签名验签服务器	安全管理区	签名验签服务器提供多种数字签名服务，包括 Attached/Detached/RAW 签名验签、数字信封加密/解密、签名二维码生成、PDF 电子签章、XMLSignature 等多种签名验签及数据加解密服务，支持国密算法。	SM2/3/4	4	为访问权限控制列表提供完整性保护
8	SSL 应用安全网关	安全管理区	SSL 应用安全网关系统，通过专有技术(FastCRL、GlobalCRL、证书快速解析等等），提高了 SSL 处理效率,为用户提供完善的用户数字证书与网上应用结合的机制。提供应用系统安全发布、应用安全访问，支持国密算法。	SM2/3/4	1	配合 PC 端部署的安全浏览器，实现 PC 端到服务端之间数据传输机密性保护
9	日志安全管理系统	安全管理区	日志安全管理系统,支持与签名验签系统对接,实现对网络中设备、系统等日志的安全管理、保障日志的完整性。	SM2/3/4	1	对日志记录进行完整性保护
10	数据加密系统	安全管理区	数据加密系统,支持对数据库数据加解密,基于透明加密技术实现关键数据加密存储,保障关键数据的机密性完整性	SM2/3/4	1	对关键数据进行机密性完整性保护

6.4. 第三方验收测试服务

1．在系统最终验收前，聘请第三方验收测评机构对横琴粤澳深度合作区行政事务局公文辅助 AI 系统（2025 年）项目进行验收测评。

2．验收测评机构依照相关政策文件出具测评结果，为系统验收提供依据，对测试中发现的缺陷和不足，提供修改意见，并进行回归测试并出具相关文档，确保项目达到与其设计结果。

验收测评的主要服务内容包括：

验收测试：依据信息系统工程项目合同、用户需求说明书以及国家相关法律法规、标准和行业规范等对信息系统的功能、性能、可靠性、易用性、维护性、可移植性等特性进行严格的测试，为系统验收提供依据，对测试中发现的缺陷和不足，提供修改意见，完善系统功能和性能。

回归测试：对未通过测试的，在修改后再次进行重新测试，以验证原来存在的问题已修改，同时确认所做的修改没有引入新的缺陷。

文档审核：对工程项目中的相关文档进行审核，并提出修改意见，便于信息系统的使用、维护。

3．验收测评服务的主要交付成果为验收测评报告。

4．验收测评服务包含在本项目采购范围内。

6.4.1. 验收测评目标

在项目验收测评等方面引入独立的第三方测评服务资格服务单位，开展信息化服务项目验收前的第三方测评及符合性检查服务等工作，严格管理项目质量，保证各项指标符合合同、需求规格说明书等设计标准和建设规范。

通过组织验收测评服务商对项目进行验收测评，及时发现建设项目中存在的质量问题及安全漏洞，协助项目业主单位解决问题，提高建设项目质量及信息系统安全保障能力，规范项目验收流程，从而达到加强项目管理的目的。

6.4.2. 验收测评依据

参照《粤府办〔2019〕2 号：广东省人民政府办公厅关于印发广东省省级政务信

息化服务项目管理办法（试行）的通知》等文件要求，通过组织第三方测试机构对本项目进行项目验收测评，规范项目验收流程，及时发现工程项目建设过程中存在的质量问题和安全漏洞并进行整改。

6.4.3. 验收测评对象

本项测评对象主要包括本项目的软件开发服务。

6.4.4. 验收测评方法和使用工具

验收测评使用黑盒测试方法，也称功能测试或数据驱动测试。它在已知产品应具有的功能条件下，通过测试来检测每个功能是否都能正常使用。在测试时，把程序看作一个不能打开的黑盒子，在完全不考虑程序内部结构和内部特性的情况下，测试者在程序接口进行测试，它只检查程序功能是否按照需求规格说明书的规定正常使用，程序是否能适当地接收输入数据并产生正确的输出信息，并且保持外部信息(如数据库或文件)的完整性。黑盒测试法注重于测试软件的功能需求，主要试图发现几类错误：功能不对或遗漏、界面错误、数据结构或外部数据库访问错误、性能错误、初始化和终止错误。测试工具包括：

web 功能测试工具：Selenium、WatiJ、WatiN、WariR、Canoo WebTest；

Windows 客户端程序测试工具：AutoIT、Twist、AutoHotKey、Abbot、Squish、STAF 等。

6.4.5. 验收测评内容和指标

测评机构在验收过程中作为独立的第三方机构，应对其实施测评的信息化项目进行客观、专业的测试，并提供权威的测评结论。应遵照有关规定规范，制订服务项目的测评方案，并根据测评方案中规定的指标和评判标准对指定测评对象（包括软硬件）实施检测，包括但不限于建设内容检查、应用系统、信息资源共享、公共信息平台等不同类型项目的测评，国（地）标等信息化标准审核、“数字政府”总体设计架构符合性审核等工作。在实施检测前与实施检测后分别提交详细的服务测评方案（包括对每种测评类型所采用标准、检测方法和检测工具的详细描述）及第三方测评报告，服务验收测评报告中应包括服务符合性检查的所有内容。

建设内容检查服务。包括但不限于以下工作：对照审核意见和立项方案备案稿逐项核查项目内容完成情况、检查项目管理是否规范、检查项目管理档案是否完整。

应用系统测试。包括但不限于以下工作：功能测试、安全性测试、可靠性测试、性能测试、容错性测试、回归测试、可维护性测试、可移植性测试、易用性测试、适应性测试、接口测试、用户文档测试。

信息资源共享测试。包括但不限于以下工作：完整性、一致性、准确性检查，内部数据库整合检查、数据格式规范性检查、信息资源目录注册完整性检查、共享信息资源提供检查、共享信息资源应用检查。

公共信息平台测试。包括但不限于以下工作：信息门户测试、公共云平台测试、应用支撑平台测试、服务接口测试。

国家或省各项信息化建设标准审核。包括但不限于以下工作：根据国家及省相关标准规范，检测并审核信息化项目建设是否满足相关标准。

“数字政府”总体设计架构符合性审核。包括但不限于以下工作：审核项目技术架构、技术路线等是否满足省“数字政府”总体设计架构和思路等。

测试方法的响应情况。包括但不限于以下工作：检查各项测试内容所参照的技术标准的完备性，测试方法的规范性。

测试工具的配备情况。包括但不限于以下工作：检查各项测试内容使用的测试工具的齐备性和充分性。

项目主管部门对测评服务开展相关工作实行服务质量考核，对其工作质量进行评价考核监督。考核内容包括但不限于以下要点：

（1）验收测评服务商应接受项目主管部门管理。

（2）根据验收测评服务商派出的服务人员的工作绩效进行评估，评估内容包括：人员的工作态度、质量控制、进度控制、安全控制效果、服务成果（包括所编制或协助编制的文档质量）、工程协调能力、遵章守纪等方面，由验收测评服务商自评及项目主管部门指定人员对验收测评服务商进行考核。

（3）对已结束的测评项目的工作质量及工作成果进行评估。

（4）对于测评服务过程中出现重大违规事件的（如违反保密协定、没履行测评

责任等），项目主管部门有权单方面终止验收测评服务商的服务资格。

项目业主单位如对验收测评服务商的服务质量不满意，可在测评项目结束后 5 个工作日内以书面形式向项目主管部门进行投诉，项目主管部门将对投诉内容进行核实，若测评机构在一个年度内经核实有效的投诉达 3 次，项目主管部门将取消其验收测评资格。

6.4.6. 验收测评结论

（1）项目承建方完成服务实施后，向采购人及其委托的监理单位提交服务实施完成报告和服务交付申请报告；

（2）采购人及其委托的监理单位审核通过服务交付申请报告之后，公平公正地选择入围的第三方测评机构，并下达服务委托书；

（3）第三方测评机构接受到测评服务委托书之后的 7 日内提交测评方案，包含测评工作计划；

（4）测评机构开展服务验收服务性检查、测评工作，并最后提交符合性检查报告（含符合性检查的所有内容）和第三方测评报告；

（5）测评工作完成后，由采购人定期对第三方测评服务进行检查和评价，并最后进行测评完成确认。

（6）由采购人及测评机构在测评服务完成报告（表）上签字确认，作为测评完成的标志，测评服务完成报告（表）作为测评服务费用结算的依据。

第七章 数据资源梳理

7.1. 数据需求目录清单

表 本项目的数据需求目录清单

序号	该数据的来源部门	该数据的来源业务系统	数据类名称	包含的数据项	数据接入方式	该数据需求涉及的业务或功能
1	行政事务局	电子公文系统	用户身份数据	账号、姓名、用户来源 id、性别、归属部门、角色、邮箱、手机号码	系统直接对接	用户通讯录，用于与统一身份认证系统对接，包括用户认证服务、用户添加、删除、修改信息
2	行政事务局	电子公文系统	粤政易登录数据	Code、token 用户 ID	系统直接对接	单点登录，与粤政易平台的用户认证服务、登录
3	行政事务局	电子公文系统	账号权限数据	用户 ID、身份、类型、文件权限数据	数据提供方	与粤政易平台的用户认证服务、登录
4	行政事务局	电子公文系统	文件数据（通过电子公文系统）	文件总数、批次号、创建时间、厂商来源、传输类型、公文元数据、文件类编码、入库位置集合、推送方的公文唯一原 id、主体公文全名、主体公文路径、公文标识、文种、份号、	系统直接对接	用于政务公文数据的标准、入库和便捷查询

序号	该数据的来源部门	该数据的来源业务系统	数据类名称	包含的数据项	数据接入方式	该数据需求涉及的业务或功能
				密级和保密期限、紧急程度、发文机关标志、发文字号、签发人、标题、主送机关、附件说明、发文机关或签发人署名、成文日期、附注、抄送机关、印发机关、印发日期、发布层次、附件文件列表信息、附件文件全名、附件路径、附件文件类型、审批意见、意见内容、审批人、审批时间、审批（人）部门、流程环节（节点）、权限集合、公文公开范围类型、公开范围详情、可见范围具体类别、主件 AI 元数据、主题词、实体日期实体地点、实体人物、实体机构、拓展元数据等		

7.2. 数据资源梳理与挂接

项目立项申报部门应结合本项目的服务内容及业务系统的功能，在数据资源方案中描述本项目拟/已产生的数据资源内容，编制数据资源目录。已建系统的可共享数据资源需完成编目挂接，不予共享数据资源需录入负面清单。产生的数据资源目录清单样表如下：

表 2 本项目产生的数据资源目录清单

序号	该数据类的生产业务系统	数据类名称	包含的数据项	采集方式	共享类型	开放类型	敏感级别	数据类型	数据范围	备注
1	人工智能平台	用户统计概览数据	用户登录量 月会话量 智能应用活跃量	数据汇聚	有条件共享（需数源单位审批）	有条件向社会开放（需数源单位审批）	1 级	库表	广东省	
2	人工智能平台	智能应用累计使用情况数据	使用人数、使用次数、token 消耗	数据汇聚	有条件共享（需数源单位审批）	有条件向社会开放（需数源单位审批）	1 级	库表	广东省	智能问答、搜索、写作
3	人工智能平台	系统监管数据	访问量、阅读量、检索量、下载量、分享量、文件入库量、阅读排行	数据汇聚	有条件共享（需数源单位审批）	有条件向社会开放（需数源单位审批）	1 级	库表	广东省	
4	人工智能平台	常规数据	入库数量、日访问量、标签数量	数据汇聚	有条件共享（需数源单位审批）	有条件向社会开放（需数源单位审批）	1 级	库表	广东省	

序号	该数据类的生产业务系统	数据类名称	包含的数据项	采集方式	共享类型	开放类型	敏感级别	数据类型	数据范围	备注
5	人工智能平台	其他数据	日志数据、敏感词数据、校对词库数据	数据汇聚	有条件共享（需数源单位审批）	有条件向社会开放（需数源单位审批）	1级	库表	广东省	

填写说明：

1.该数据的生产业务系统：目前生产该数据类的业务系统名称，系统需在项目管理系统注册登记。

2.数据类名称：本部门数据资源目录中涉及的具体数据类别，以业务为主题进行划分，即系统数据库设计文件中定义的数据表。数据类名称命名规范如下：

（1）数据名称填写基本原则遵循：“数据范围+数据主体+业务（行为）属性”，命名样例如下：

① 合作区医疗机构医疗资源情况；

② 合作区社会团体法人登记证书；

（2）一个部门架构下禁止存在相同名称的目录名称；

（3）多个目录意义相近的，目录名称需要明确区分；

（4）一般禁止使用符号，特殊符号；

（5）不影响表义的情况下，尽量使用对应的中文表达英文词串含义，并根据不同的数据类型完成数据的编目。

3.包含的数据项：数据类中涉及的数据项业务含义的详细数据字段清单，并请按照《广东省数据资源“一网共享”体系公共数据元规范》规范公共数据元的采集和使用。

4.采集方式：明确数据源的采集方式，主要包括人工采集、终端采集、数据汇聚（不限于一种）。

①人工采集：通过在线填报、手动录入、人工导入等方式采集数据，如问卷调查、

实地调研、资料分析等产生的数据，以及通过移动介质拷贝的数据，包括常用的文件交换类型和数据库导出文件；

②终端采集：通过摄像头、无人机、传感器等终端设备获取数据；

③数据汇聚：通过系统库表交换、数据接口、文件交换等方式获取数据。

5.共享类型：明确是否可以共享，包括无条件共享（仅对政府内部）、有条件共享（需数源单位审批），不予共享。

6.开放类型：明确是否可以开放，包括不向社会开放、有条件向社会开放（需数源单位审批）、无条件向社会开放。

7.敏感级别：按照《广东省数据资源“一网共享”平台数据资源分类分级指南》，从影响对象和影响程度要素进行定级:

①1 级：对国家安全、经济运行、社会稳定、公共利益、组织权益和个人权益无危害；

②2 级：对公共利益、组织权益和个人权益造成轻微影响，且结果可以补救；

③3 级：有下列情况之一：对公共利益、组织权益和个人权益造成一般影响，且结果可以补救；对经济运行、社会稳定造成轻微影响，且结果可以补救；

④4 级：有下列情况之一：对公共利益、组织权益和个人权益造成严重影响，且结果不可逆但可以采取措施降低损失；对经济运行、社会稳定造成一般影响，且结果可以补救；对国家安全造成轻微影响，且结果可以补救。

8.数据类型：包括系统库表、服务接口、文档、音视频、压缩包、电子证照、地图产品等。

9.数据范围：是指数据适用的地理范围。

10.备注：有条件共享和不共享的法律法规依据及政策理由，详细说明该数据类纳入共享负面清单的原因或依据，有明确条款规定的应列出来源及条款内容。

（1）有条件共享的法律法规依据和政策理由主要包括：

①如写明申请部门业务对该类数据的共享需求是依于哪条法律、法规和政策或者依据哪份函件，在某某应用场景下需要的，可同意共享；

②如写明申请部门的业务需求属于数据统计和分析，对具体数据项明细无需求的，

可同意共享该类数据的统计结果；

③如写明申请部门业务属于某一特定业务场景或者特定行业的，可同意共享；

④各部门须明确的其他符合规范要求的具体条件。

（2）不予共享的法律法规依据和政策理由主要包括：

①各单位涉及国家秘密、国家安全的业务数据，不能够在政府内部共享，不进行共享；

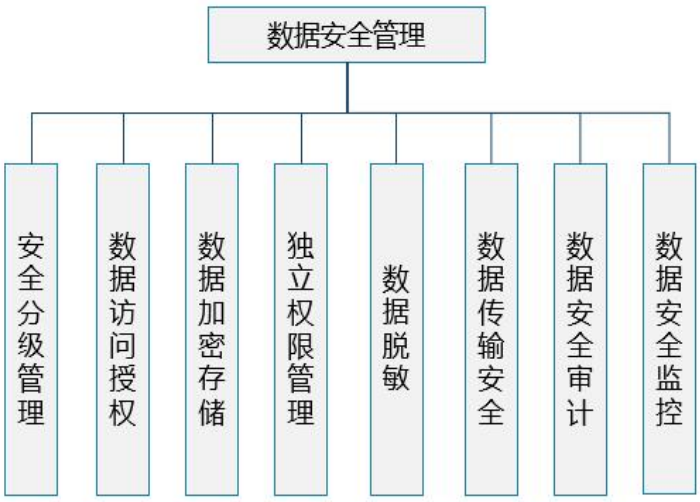
②各单位有法律、法规、规章依据明确规定，不能在政府内部共享的业务数据，不进行共享；

③其他不能共享的政策理由。

7.3. 数据安全

数据安全管理依据国家、行业相关法规制度，制定合理、科学的数据安全分级标准，并通过数据授权访问机制规范数据的存储和使用。数据安全管理的工作目标是保证业务数据使用的安全性和合规性。

数据安全管理应用设计如下图所示：



数据安全管理应用设计图

7.3.1. 安全分级管理

根据一系列的数据安全分级标准和政策，定义数据安全级别，为数据应用以及数据管理中实施数据安全保护和访问提供数据安全控制的基础。

7.3.2. 数据访问授权

定义用户所属的角色或者功能，明确各类用户能够访问的数据范围，并按照角色或功能指定可以访问的数据对象。结合 LDAP 和双因素等方式，建立统一认证体系，将所有用户认证取值全部交由统一认证体系完成。

7.3.3. 数据加密存储

1.数据完整性

（1）基本要求

能够检测到重要用户数据在传输过程中完整性受到破坏。

能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。

能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

（2）实现方式

通过使用 Hash 校验的方法确保数据的完整性。

传输过程的完整性受到损坏则采取数据重传的机制。

对于存储的数据则应采取多个备份的方式，防止单一数据损坏造成的损失。

2.数据保密性

（1）基本要求

采用加密或其他保护措施实现鉴别信息的存储保密性。

采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性。

采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

（2）实现方式

无论在身份验证阶段还是数据传输阶段都使用加密的形式传输数据，通常的方法

可以使用 SSL 或 TLS 等方式，也可以使用 VPN 或专用协议传输；

对存储的重要数据需要采取加密手段进行保存；

对于本身就是加密方式存储和使用的数据，在传输过程中可以适当降低对传输过程中加密的要求。

（3）部署方式

通过依托用户的 CA、VPN 方式实现。

通过采用支持国密标准方式的本地存储实现。

3.安全管理

需要为本项目建立一套安全管理体系、规章制度。

以确保所有数据的安全，任何用户不能直接存取本系统数据库数据。

数据库敏感数据（密码等）要求加密处理。

必须确保数据接口的安全，不能破坏其他运营系统数据。

确保数据传输安全。

7.3.4. 独立权限管理

该模块实现基于密文的增强访问权限控制，防止 DBA 及高权限用户对敏感数据进行访问。所有数据库用户想访问密文数据，必须经过密文授权。

7.3.5. 数据传输安全

为防止数据传输过程被截获、篡改，建议采用加密的技术对传输的敏感数据进行数字签名和加密。

1.数字签名

数字签名是用于在数字化文档上的身份验证技术，签名是不可伪造的。

2.数据加密

对于十分重要的数据，系统可采用国密算法进行数据加密。

3.数据传输加密的技术实现

Tuxedo 支持链路层安全机制，包括了身份验证、授权和链路层加密（LLE），有效确保了 BEA Tuxedo 应用在跨网络部署时的数据隐私。它的实现也非常方便只要设

置一个系统级参数，就可保证消息在传输过程的加解密自动处理。

同时 Tuxedo 还支持公钥加密、数字签名和第三方安全产品集成。

7.3.6. 数据安全审计

提供访问记录追踪处理，系统具有安全审计功能。通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括：根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等；对安全审计员进行严格的身份鉴别，并只允许其通过特定的命令或界面进行安全审计操作。

具体集中审计内容包括：

1.日志监视

实时监视接收到的事件的状况，如最近日志列表、系统风险状况等；监控事件状况的同时也可以监控设备运行参数，以配合确定设备及网络的状态；日志监视支持以图形化方式实时监控日志流量、系统风险等变化趋势。

2.日志管理

日志管理实现对多种日志格式的统一管理。通过 SNMP、SYSLOG 或者其它的日志接口采集管理对象的日志信息，转换为统一的日志格式，再统一管理、分析、报警；自动完成日志数据的格式解析和分类；提供日志数据的存储、备份、恢复、删除、导入和导出操作等功能。日志管理支持分布式日志级联管理，下级管理中心的日志数据可以发送到上级管理中心进行集中管理

3.审计分析

集中审计可综合各种安全设备的安全事件，以统一的审计结果向用户提供可定制的报表，全面反映网络安全总体状况，重点突出，简单易懂。

系统支持对包过滤日志、代理日志、入侵攻击事件、病毒入侵事件等十几种日志进行统计分析并生成分析报表；支持按照设备运行状况、设备管理操作对安全设备管理信息统计分析；支持基于多种条件的统计分析，包括：对访问流量、入侵攻击、源地址、用户对网络访问控制日志等。对于入侵攻击日志，可按照入侵攻击事件、源地址、被攻击主机进行统计分析，生成各类趋势分析图表。

系统可以生成多种形式的审计报表，报表支持表格和多种图形表现形式；用户可以通过浏览器访问，导出审计结果。可设定定时生成日志统计报表，并自动保存以备审阅或自动通过邮件发送给指定收件人，实现对安全审计的流程化处理。

7.3.7. 数据安全监控

根据安全分级授权访问清单对执行情况进行严格监控，定期出具安全检查报告。

7.3.8. 数据库安全管理

针对数据库的安全从以下几个方面入手，内容如下：

1.定期备份数据库

任何系统都有可能发生灾难。服务器、数据库也会崩溃，也有可能遭受入侵，数据有可能被删除。只有为最糟糕的情况做好了充分的准备，才能够在事后快速地从灾难中恢复。把备份过程作为服务器的一项日常工作。

2.禁用或限制远程访问

首先要避免从互联网访问数据库，确保特定主机才拥有访问特权，需要指定的 IP，如果使用了远程访问，要确保只有定义的主机才可以访问服务器。

3.设置 root 用户的口令并改变其登录名

在 linux 中，root 用户拥有对所有数据库的完全访问权。因而，在 Linux 的安装过程中，一定要设置 root 口令。当然，这是需要使用强口令来避免强力攻击。为了更有效地改进 root 用户的安全性，另一种好方法是为其改名。为此，你必须更新表用户中的数据库。

4.移除匿名账户和废弃的账户

有些数据库的匿名用户的口令为空。因而，任何人都可以连接到这些数据库，我们可以移除匿名账户和废弃的账户，以避免不必要的访问。

5.降低系统特权

常见的数据库安全建议都有“降低给各方的特权”这一说法。一般情况下，开发人员会使用最大的许可，不像安全管理一样考虑许可原则，而这样做会将数据库暴露在巨大的风险中。为保护数据库，务必确保真正存储数据库的文件目录是由“数据库”

用户和“数据库”组所拥有的。

6.降低用户的数据库特权

有些应用程序是通过一个特定数据库表的用户名和口令连接到数据库的，安全人员不应当给予这个用户完全的访问权。如果攻击者获得了这个拥有完全访问权的用户，他也就拥有了所有的数据库。为定义用户的访问权，使用 GRANT 命令。如此一来，user1 用户就无法改变数据库中这个表和其它表的任何数据。

7.安全补丁

务必保持数据库为最新版本。因为攻击者可以利用上一个版本的已知漏洞来访问企业的数据库。

8.数据完整性和一致性保护

系统采用了多种保护手段，确保数据完整性和一致性。既在服务器端通过完整性约束、触发器等方法进行保护，又在客户端应用程序中通过检查输入数据的有效性加以保护。

第八章 项目建设及运行管理

8.1. 领导和管理机构

根据项目管理规范，应严格按照项目组织机构设置的原则建立项目组织机构，满足整个项目已明确的需求与可能存在的期望。

1、项目领导小组

项目设置项目领导小组作为整个项目的决策机构与总指挥，负责制定项目策略和目标，调配各方人力，明确各方职责和权力，监控整个项目的实施过程。

2、项目经理

项目经理由项目领导小组任命，应由懂技术、懂业务、有协调能力的人员担任，是该项目实施的具体管理者和控制人。项目经理负责制定实施计划，组织和指导具体执行项目工作，同时其必须随时了解项目实施的情况，并对项目质量负责。

3、项目执行小组

项目执行小组是具体项目实施机构，主要承担工作包括：

（1）对项目进行详细周密的设计，并制定项目质量保证书。

（2）进行项目的具体实施。

（3）做好项目的后勤保障，保证项目建设资源的合理与充足。

（4）及时、主动在项目实施关键节点，或根据项目要求定时向项目领导小组提交项目所需的进度报告、数据统计报表等文件。

（5）做好项目在进度、成本、质量控制，以合同为基准及时纠正项目建设中存在的问题。

（6）项目实施完成后，及时提交项目测试申请报告，并及时改进发现问题。

（7）负责系统试运行和上线工作。

（8）做好项目管理及培训工作。主动做好人员培训，制定操作规程及规章制度；建立项目档案制度，保证项目资料的完整。

8.2. 运行维护方式

系统建成后，合作区行政事务局承担项目运行维护工作的总体管理职责，具体运

维实施由行政事务局相关信息化服务团队负责，局办公室、业务部门、承建方及运维服务商具体落实。

1、项目交付

系统验收完毕，项目承建方向合作区行政事务局移交项目，同时移交相关文档，如：

开工报告、合同、招标文件、投标文件、中标通知书；

实施方案；

需求规格说明书；

概要设计说明书；

详细设计说明书；

软件开发项目计划；

数据库设计说明书；

系统部署方案、部署手册；

系统自测方案、系统自测报告；

项目初验报审表、初验方案、初验会议纪要、初验报告；

试运行方案、试运行记录、试运行报告；

培训方案、培训记录、培训签到表、培训效果反馈表；

总结报告；

验收汇报 PPT 资料；

用户使用报告；

管理员手册；

用户使用手册；

竣工验收意见；

系统移交清单；

资料移交清单；

承建单位周报（月报）；

变更情况说明、变更记录。

在项目移交后，系统进入运行维护阶段，将由承建方提供的技术支持和维护计划，并提供相应的信息安全服务，以确保系统的正常运行。

2、维护内容

系统项目承建方应提供 1 年的维护保证期，包括 5×8 小时的现场工作日服务、非工作日 8 小时值班应急响应服务。

（1）技术服务内容

技术服务内容包括：错误修改、轻量级需求变更、性能优化、运行环境诊断及保障，以及由于技术规范变化导致的程序变更。

开发建设过程中，建设单位要与需求单位密切配合，共同规划系统整体架构、数据库设计、业务功能模块开发等建设内容，共同研究制定业务应用、安全管理以及与其他相关系统的对接实施方案。

（2）提供详细的维护人员清单

承建方应提供本地化技术服务队伍承担系统的技术服务工作，需向用户提供详细的维护人员清单及其联系方式，主要维护人员要保持稳定。

（3）预防性维护

承建方应提供预防性服务，在服务的过程中，培训使用单位的技术人员执行预防性维护任务。

8.3. 项目招标方案

本项目采用财政性资金建设且预算金额在采购限额标准以上，根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》等相关政策法规，本项目建设内容将采用委托招标的组织形式和公开招标的招标方式，委托具备相应资格的政府采购代理机构（或集中采购机构）进行公开招标。

8.4. 项目建设周期

建设周期为 6 个月。

8.4.1. 项目具体实施进度、质量、资金管理方案

项目具体实施进度

项目期建设分为以下几个阶段：

1、项目准备阶段

本阶段主要完成本项目的立项申报及审批工作，落实项目建设资金，完成项目招投标准备工作，预计为期 1 个月。

2、项目实施阶段

本阶段主要完成系统设计、应用系统开发、软件采购和部署实施等工作，并完成现有数据迁移、数据格式转换等基础性工作，预计为其 3 个月。

3、项目试运行阶段

本阶段主要完成项目整体试运行，修正项目各组成部分联调中出现的问题，修正软件 bug。试运行期为 3 个月，试运行期无重大故障且解决所有发现的缺陷后进行项目整体验收。

4、项目验收阶段

根据市财政资金项目竣工验收的相关要求，开展项目第三方测评、项目内部验收、竣工验收等工作。本阶段在项目试运行期同步开展，试运行期结束后进行项目验收。项目验收阶段预计为期 1 个月。

8.4.2. 项目质量管理方案

为了保证本次项目建设的质量，需严格按照项目质量管理和质量保证体系的相关要求，制定详细的项目进度计划和质量保障措施，确保项目按期保质完成。

以下从项目实施各个阶段来规划项目质量管理工作。

1、前期工作阶段质量管理

前期工作的质量是整个项目的关键，处于十分重要的地位。需要建立项目质量管理责任制，制定项目质量计划。

（1）建立项目质量管理责任制

项目经理是项目前期工作质量的全权责任人，要亲自抓质量工作，并且还配备了质量管理人员协助工作，主要任务包括：

在编制项目前期工作计划的同时，明确各项前期工作的质量要求，制定分层次的质量职责，制定质量计划并组织实施；

按质量计划规定，督促、检查项目质量计划执行情况，特别是主要质量控制点的验证、检查和评审活动；

发现调查研究不细，数据不实，分析方法不科学、不合理，不符合有关规定时，要认真组织补做有关工作。

（2）制定项目质量计划

识别用户方的要求和期望，明确成果的质量目标和质量标准。

把质量目标要求层层分解，按质量计划和实施步骤层层落实，一直落实到个人，使每一层次的职责、权限、资源分配以及保证质量的措施都予以明确。

在质量计划中，要明确影响质量的控制节点，以及如何进行质量检查、控制。

质量管理计划繁简程度应与项目要求及项目组织的运作方式相适应。

在计划执行中，要不断反馈执行信息，及时解决执行中出现的问题。

2、项目设计阶段质量管理

设计阶段的质量控制是要追求质量的优良化。即在一定投资限额约束下，能达到所需要的最佳功能和较高质量水平。

项目设计阶段要对以下内容进行质量控制管理。

对设计全过程进行管理，监督检查设计质量体系文件、项目质量计划的执行情况；

根据项目计划、项目质量计划和设计计划的规定，对设计过程进行控制；

确定设计输入并组织对设计输入的评审，确认其适用性和完整性，审查其内容是否满足设计要求；

各组织接口和技术接口，要能组织协调；

对设计方案进行审查和协调，确保方案的合理性；

组织和监督设计各阶段的设计评审和设计验证；

控制好设计变更控制程序；

对设计关键控制点进行检查，组织或检查对设计质量有重大影响的活动和设计文件。

3、项目实施阶段的质量管理

项目实施阶段要做如下的质量控制活动：

根据项目的特点，制定调整实施阶段的项目质量计划，将实施阶段的项目质量目标层层分解、层层下达、层层落实，落实到每个实施组别，落实到个人，使每个人都了解完成本职工作的质量要求和具体质量标准，明确自己的努力方向。

确定过程质量控制点、质量检验标准和方法。

按质量计划实施过程控制，前后实施阶段间要有交接确认制度。

对项目实施各阶段的成果进行评审。

4、试运行阶段质量管理

试运行是对设计和实施等工作质量的综合考核，是对项目质量的最终检验和试验。试运行质量管理的目的是要确保试运行成功，达到合同规定和设计要求。具体的工作包括：

试运行操作和合格标准应遵循和符合试运行方案的规定。

试运行的风险大，必须循序渐进，不具备条件不得试运行。

发生事故后，试运行指导人员应果断处理，防止事故扩大，并及时提供事故报告。

5、运行维护阶段质量管理

运行维护阶段质量控制主要从以下几方面来完成：

定期对运行维护状态进行监控和管理。

对项目变更进行记录并根据质量体系进行质量控制。

对运行维护中出现的问题进行监控，并对问题修复状态进行管理。

对运行维护阶段新编制的成果组织进行评审。

8.4.3. 项目资金管理方案

按照专人管理、专款专用、预算控制等原则，建立项目资金使用台账，采用专款专人管理的方式，严格、规范开展资金预算、计划、控制、分析及核算工作，确保项目资金预算的合理、合规使用。

8.5. 相关管理制度

本项目建设将实行项目管理制度，项目管理将遵照执行国家、省、市对项目实施流程、招标采购、质量控制、安全防范等做出的相关规定。项目管理的程序将包括组

织和人员建设、需求分析与调研、解决方案确定、实施计划、测试培训和验收等各个阶段。

8.6. 用户培训

8.6.1. 培训目的

培训在本项目中的重要意义主要体现在以下几个方面：

1、保障系统正常运行：由于本项目是关系到横琴粤澳深度合作区行政事务局公文辅助 AI 系统的畅通运行，其运行质量关系重大，需要建设有经验、专业化的技术队伍。这支队伍的职责主要体现在日常的系统管理、运行维护管理当中。这些任务要求技术人员具有较高的技术技能，有必要对他们进行专门的技术培训。

2、培养各级管理和应用人才：通过进行系统的培训，可以使各级人员掌握系统的各类产品和应用系统的功能和性能：对于一般操作人员，可以熟悉各新增子应用系统的基本功能，方便进行工作；对于系统的运行维护人员，可以了解系统的具体特点和维护方法，熟练的进行系统的维护操作，对于系统管理员，可以方便地对系统进行科学地管理。

8.6.2. 培训计划

针对业务操作人员的培训内容主要是针对各自负责的业务系统业务功能和业务操作方面的培训。包括：对所有与应用系统相关的工作人员进行完整的使用和操作培训。

根据本项目特点，业务人员培训工作将分阶段实施，循序渐进。在项目的实施过程中，人员培训是非常重要的一个环节，人员培训质量的好坏，将直接影响项目实施的进度和实施质量。根据用户的关注点和在系统中的应用层面不同，要进行针对性的培训，同时将所有用户对象进行分层次培训，分为以下三个层次：

1.基础用户（普通公文起草人员），培训重点：新功能的基本操作、常见问题解答。培训时长：1 小时/次。

2.高级用户（公文审核岗位、综合处室），培训重点：新功能的深度应用、与其他系统的协同使用。培训时长：2 小时/次。

3.管理员（系统维护人员），培训重点：新功能的配置管理、权限设置、日志查看。培训时长：1.5 小时/次。

8.6.3. 培训内容

1.功能更新说明，介绍新功能的背景、目标及适用场景（如“政策术语智能校验”功能适用于公文审核场景）。展示功能操作界面及核心操作步骤（如“如何调用新模板库”）。

2.实操演练，提供模拟公文场景（如起草一份《跨境金融政策通知》），引导用户完成新功能全流程操作。针对常见问题（如“如何调整模板格式”）进行现场演示与解答。

3.案例分享，讲解其他政府单位使用新功能的成功案例（如“某局通过智能校对功能将审核耗时缩短 50%”），提供最佳实践指南（如“如何高效使用素材推荐功能”）。

第九章 项目效益及风险分析

9.1. 效益分析

9.1.1. 社会效益分析

公文辅助 AI 系统的应用，将为本单位带来重大的社会效益，将形成深远影响。一是基于国产化操作系统、数据库、CPU/GPU 的人工智能平台，通过有效地规范的安全防护措施，提升了信息安全水平、智能化水平，有效杜绝重大安全事件的发生，减少潜在的社会隐患。二是有效提高机关业务规范程度和信息化水平。通过顶层设计和项目实施，统筹汇聚各部门间的公文，避免信息孤岛。同时，提高了机关业务人员办文的规范度，提高工作效率。三是培育大模型应用土壤，通过政务大模型在数字政府中的应用，深化大语言模型的应用场景、积累模型语料、调优算法、培养使用习惯，为大语言模型在交通、医疗、教育、科技等领域的应用培育土壤，扶持人工智能产业发展。

9.1.2. 经济效益评价

打造人工智能平台，以自动化流程加快工作速度，自动处理重复性任务，如数据录入、文件分类等，减少人工操作，优化资源分配和任务安排，提升整体运营效率，对单位日常工作产生的文件数据进行统一的分类、整理、归集，形成单位内部的智能办公工具，提升单位内部用户对文件数据的利用效率，解决之前文件找不到，或者检索的文件匹配度低的问题。通过智能化的手段，实现了对各类文件数据的快速处理与分析，使得政府能够更加精准地掌握各类信息，为决策提供了科学依据，提升工作人员日常办公的效率，也为领导决策提供了有力的数据支撑，支撑数字政府的高效运转，提升政府治理水平。

9.2. 风险分析及对策

9.2.1. 技术风险

主要体现在业务系统的多样性，可能造成系统接口复杂；另外负载估计不准确，可能造成数据分析服务的性能瓶颈。

正对接口复杂和多样性，采用两个主要措施进行规避。一是按照既定的标准和规范统一建设接口系统；二是降低系统之间的耦合度，明确采用数据级整合方式实现松散耦合。

针对负载估计不准造成性能瓶颈，采用储备备用资源方式，在存储、交换方面都预留一定的应急储备。

9.2.2. 安全风险

由于数据处理的特殊性，安全问题是一个非常关键的问题，如果安全管理跟不上，就可能造成数据的滥用，个人隐私泄露等。

针对安全隐患，从法规和技术两个方面实现保障。首先在法规上，要制定数据管理办法，在数据获取的情况下，保证数据的安全管理和合法使用。其次在技术上要构建安全保障体系，从物理层、网络层、系统层、应用层和数据层各个层面进行安全防护。

9.2.3. 实施风险

针对项目实施风险，一方面要加强沟通和协调，提高业务部门对项目的认识；另一方面对平台对接目标可以从低到高，首先是从业务流程单纯、简单的业务归口部门的集成，然后再逐步扩展至所有单位，这将减少实施的实际难度和复杂程度。

9.2.4. 管理风险

建设期间内主要体现在关联项目多、项目管理难度大。建设完成后可能存在管理部门不明确或者权重不匹配，造成运行管理困难。

针对管理风险，关键在于运行机制，为此应尽快制定并颁布相关的标准规范，明确管理职责和分工。

第十章 项目进度计划

10.1. 项目实施机构

本项目由横琴粤澳深度合作区行政事务局组织实施建设。

10.2. 项目工期

1.项目周期

项目周期为建设期 6 个月，后续为 12 个月的运维运营期。

10.3. 项目实施计划

本服务项目里程碑计划如下：（T 表示项目合同签订日期）

序号	工作内容	里程碑事件	时间
1	项目启动	项目正式启动	T+1d
2	需求调研	调研报告	T+30d
3	需求分析	确认业务需求说明书	T+60d
4	系统开发	完成系统主体功能开发	T+90d
5	功能测试	完成主体功能测试报告	T+120d
6	部署上线	完成系统试运行	T+150d
7	系统完善和优化	完成缺陷修复及功能优化	T+160d
8	系统正式上线	建设期完成，进入运营期	T+180d
9	系统运营	运营运维	T+540d

10.4. 项目进度控制

10.4.1. 项目进度控制目的

项目进度控制和监督的目的是：增强项目进度的透明度，以便当项目进展与项目计划出现严重偏差时可以采取适当的纠正或预防措施。已经归档和发布的项目计划是

项目控制和监督中活动、沟通、采取纠正和预防措施的基础。

10.4.2. 项目进度控制措施

为了确保项目按期完成，必须对项目的进度进行持续的监控管理。通过制定项目计划和对计划的定期回顾检查，按照一定的汇报机制，管理项目的执行情况，并根据实际情况，对项目计划进行必要的调整。我们所建议的进度控制主要手段包括：

10.4.2.1. 项目例会

由项目经理定期召集举行项目例会，对项目的实施工作完成情况进行总结并确定下一步计划，同时在会上对提出的争议和问题进行讨论。项目例会通常参加人员是双方项目组成员（双方项目经理必须参加）。例会结束后整理《会议纪要》，发送给双方项目管理负责人。

由项目经理根据项目情况召集举行项目月度例会，主要讨论总体的项目进展、问题和变更的状态、后续的工作进程和任务分配等并形成会议纪要。参加人员是项目经理及项目组核心成员。

在实施过程中发生的临时性会议，视情况随时召集，参加人员是项目经理及项目组核心成员，结果报告双方项目总监，由双方高层协商确定。

所有会议均应在会议结束后产生《会议纪要》，通知双方的项目经理。

10.4.2.2. 项目状态报告

在项目实施过程中，项目经理根据项目的情况，应定期向软件工程部经理提交项目状态报告并抄送质量保证部经理，汇报项目的进度、质量、成本方面进展以及完成、未完成工作、存在问题、下一步的工作计划等内容，并在此基础上形成对客户方的项目状态报告，具体的格式参见相应的模版。

10.4.2.3. 项目里程碑/阶段评估验收

在项目里程碑点或者阶段点，项目经理组织双方相关人员进行评估和验收，就本阶段/里程碑完成情况进行确认，如果需要进行变更则进行沟通和协商，结束后形成《会议纪要》，并提交给双方项目管理负责人，由双方高层协商确定。

10.4.2.4. 项目审计

项目过程中，公司质量保证部 SQA 将定期或不定期对项目情况进行审计，从进度、成本、质量等方面进行报告，以第三方的形式总结项目问题，并提交《会议纪要》给公司质量保证部经理，由公司项目管理委员会。

10.4.2.5. 进度管理制度

项目就是为了实现一个独特的目的而进行的临时性任务，因此项目具备明确的时效性，项目的进度监控以及风险管理是项目成败的关键。在项目计划阶段便需要完成项目进度计划的编制，建立项目的进度监控机制以及风险的识别、量化以及应对计划。

项目进行过程中，我们通过以下制度及时通报项目的进度和风险，并积极寻求应对的办法。

10.4.2.5.1. 周例会制度

项目经理每周组织与客户方的项目组成员共同参加的周例会。在周例会上，项目经理要与客户就项目计划执行情况、项目面临问题和风险等进行沟通，并对下一个阶段的工作进行汇报，及时收集客户方反馈，采纳合理建议。

周例会除了对已经发现的问题和风险进行通报和讨论，还会运用同类项目的《会议纪要》以及“头脑风暴”等办法主动识别项目的各种存在风险。对于发生的风险，则量化后依据项目计划阶段确定的风险应对计划进行讨论，确定应变处理的方案。

10.4.2.5.2. 周报制度

项目经理在实施项目的过程中，需要以邮件的方式提交《项目情况表》，即项目计划执行情况汇报表。该周报详细记录项目的进展情况、已完成的工作、未完成的工作、存在的问题和风险，以及工作计划。通过周报制度，项目经理可以全面、系统地掌握项目的整体进度和细节，同时也方便客户方了解项目的最新动态。此外，周报还作为项目经理与项目组成员之间沟通的重要桥梁，有助于团队内部的信息共享和协同工作。对于周报中提及的问题和风险，项目经理需及时组织团队进行讨论并制定解决方案，确保项目的顺利进行。

10.4.2.5.3. 月报制度

项目经理每月组织与双方的关键项目组成员以及主管领导共同参加的月汇报会。

在月汇报会上，项目经理要与客户就项目计划执行情况、项目面临问题和风险等进行总结和展示，并对下一个阶段的工作进行汇报。以便双方领导能够了解项目的阶段成果和进行阶段性的决策。

月汇报会项目经理详细展示项目计划的实际执行情况，包括已完成的任务、里程碑的达成情况、资源的使用效率等，同时也会诚实地反映项目面临的问题和挑战，包括技术难题、资源短缺、进度延误等。对于这些问题和风险，项目经理会提供详细的分析和评估，以及已经或计划采取的应对措施。项目经理还需对下一个阶段的工作进行详细的汇报，包括计划完成的任务、预期达到的目标、需要的资源和支持等。月汇报会结束后，项目经理会根据会议讨论的结果和领导的决策，及时调整项目计划和策略，确保项目能够按照预定的目标和时间表顺利推进。

10.4.2.5.4. 关键点检查制度

制定项目计划的时候，根据项目的具体情况，双方需要确定若干个项目关键检查点（该点的项目计划执行情况对整个项目起决定性作用），当检查点到达的时候，由项目经理召集双方的关键项目组成员以及主管领导参加检查点汇报会议。双方领导根据项目计划当前执行情况以及面临的问题和风险，决策下一步的工作。在关键点检查会议上，项目经理需要详细汇报该检查点对应的项目计划执行情况，包括已完成的关键任务、关键里程碑的达成情况、资源的使用效率等。同时，项目经理也需要诚实地反映在该检查点遇到的问题和挑战，包括技术难题、资源短缺、进度延误等。对于这些问题和风险，项目经理需要提供详细的分析和评估，以及已经或计划采取的应对措施。双方领导在听取项目经理的汇报后，会根据项目计划当前执行情况以及面临的问题和风险，共同决策下一步的工作方向和重点，以确保项目能够按照预定的目标和时间表顺利推进。关键点检查制度的实施，有助于及时发现和解决项目中的问题，降低项目风险，提高项目的成功率和效率。

10.5. 项目验收流程

在系统开发、测试、实施、联调、运行后，要进行整个系统的验收。项目验收包括两个方面，一是软件系统的验收，二是对项目交付文档的验收，验收人员针对这两个成果进行评审并签署验收报告。

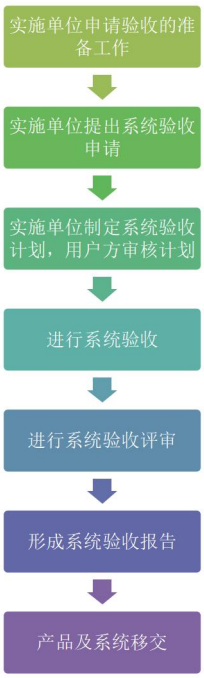


图 1：项目验收流程图

10.5.1. 实施单位申请验收的准备工作

根据横琴粤澳深度合作区公文辅助 AI 系统的特点，系统验收应在系统运行环境中进行。系统验收申请前应完成如下的工作：

实施单位应在系统交付用户方验收之前，对系统的运行情况进行确认；

实施单位在完成确认测试后，证实系统已满足合同规定的条件及需求说明书中对系统功能和性能的要求；

实施单位应准备好提交验收的各种文档、系统软硬件配置清单，并做好系统的交付准备；

实施单位的实施小组应准备好《测试分析报告》和《技术总结报告》，作为系统验收的必备文件提供给用户方；

实施单位应支持用户方对系统的验收测试和评审；

实施单位应作出向用户方提供人员培训和技术支持的计划。

10.5.2. 系统验收申请

实施单位在完成规定的系统验收申请前的各项准备工作以后，应适时向用户方正式提出系统验收申请报告，简要说明申请系统验收的准备情况和系统所具备的验收条件。实施单位在提交系统验收申请报告时，必须按合同书的有关规定，交付有关横琴粤澳深度合作区公文辅助 AI 系统升级项目的相关资料，其中包括系统设备及系统软件配置清单、文档、技术总结报告和测试分析报告等。系统验收申请报告应有实施单位的技术负责人签字。

用户方的经办人必须了解要验收系统的功能、性能和系统配置与文档等方面的要求，掌握合同书中规定的系统验收条款，对实施单位提交的系统验收。

申请报告进行审查，提出处理意见。用户方经审查后，在申请报告上签字并对实施单位的申请作出答复。用户方将按合同有关条款做好系统验收的全部准备工作，包括对测试用例、测试数据、测试过程和测试环境的准备。

10.5.3. 系统验收计划

在系统验收活动进行之前，实施单位应制定一套完整的系统验收测试计划。系统验收计划应由系统的实施单位和用户方共同制订或由用户方委托实施单位制订。该计划要由用户方认可，而且还要包括一些由用户方提供的测试方案。该计划应包括系统验收工作的活动程序、验收测试要求、技术条件、设备资源、验收准则、工作人员的组成以及日程安排等内容。该计划由用户方审定后执行。

10.5.4. 验收测试计划

系统的验收测试是系统验收活动中最关键的步骤，横琴粤澳深度合作区公文辅助 AI 系统升级项目必须满足合同条款与系统需求说明书中规定的要求。

（1）测试计划及流程包括下列内容：

1）测试计划及程序的目的；

2）各项功能测试所需输入的数据；

3）测试结果记录的说明；

4）观察、测试结果的设备、工具及程序；

5）测试进度表。

（2）有关的测试结果要以书面报告的形式由实施单位向用户方提交，内容包括：

1）测试的系统功能；

2）为纠正系统缺点需做的变动；

3）为提高系统性能提出的建议。

10.5.5. 验收测试前的检查

在系统验收测试开始之前，用户方提前将验收的有关资料分发给用户方验收人员。验收人员需要检查测试环境是否符合要求，检查全部测试项目的测试用例是否准备好，有关测试人员是否全部到位。

10.5.6. 系统演示

实施单位应向用户方演示横琴粤澳深度合作区公文辅助 AI 系统升级项目的全部界面、系统包括的主要功能、性能，以证明系统实现的功能与合同要求一致。通过演示活动让用户方成员对系统有一个直观和概括的了解。验收委员可现场选用实例对被验收系统时行演示考核，以证实与系统需求的一致性、程序和文档的一致性。

10.5.7. 验收测试

系统验收测试组应按系统验收测试计划对系统进行功能测试、可靠性测试、安全性测试、性能测试、一致性测试和文档测试。测试员按分工分别对被验收系统进行逐项测试，并详细记录每一项测试结果，将这些结果分别与预期的结果对照分析，然后写出《系统验收测试报告》，该报告将作为用户方评价系统的主要依据，也是用户方确定是否接收系统的主要依据。

10.5.8. 系统验收评审

在验收测试完成以后，用户方主持评审会，通过有关报告和审议验收结果，并对系统作出综合评价。

（1）评审内容包括：

1）《文档审查报告》；

2）《系统验收测试报告》；

3）《测试分析报告》；

4）《技术总结报告》。

（2）按以下的验收准则对系统进行评价：

系统是否满足用户信息系统要实现的目标。

系统采用的技术和实现方案是否做到可靠、稳定、灵活、实用。

所选用的应用开发平台和开发工具先进、简便、有效，便于与其他系统的衔接，实现资源共享。

运行系统的可靠性是系统建设的首要出发点。因此，要求实施单位提供高可靠性的平台和技术，确保系统的安全和可靠。要求系统具有较强的容错能力，使系统不易崩溃。

关键系统设备与数据备份的设施是否达到安全可靠。

用户方进行讨论，对被验收的系统给出实事求是的评价，内容包括系统的先进性、功能性、可靠性和安全保密性。最后由用户方进行决定系统是否通过验收。

10.5.9. 系统验收报告

在验收评审后，用户方应写出《系统验收报告》，详尽地记录验收中对系统的评价及验收意见。尤其要明确系统在验收中发现的问题和缺陷，以及需要改进的意见和实施单位对此所作的承诺。用户方全体成员在验收报告上签字。根据用户方表决情况，由用户方主任在验收报告上签署验收意见。

如果系统验收不能通过，用户方将根据合同书的规定与供需双方协商处理意见，可能的结果是：要求实施单位限期完成开发任务，重新提出验收申请或者终止合同。系统验收通过后，要确定系统进入试运行的时间结束时间，明确实施单位在试运行期间要解决的遗留问题以及改进系统的意见，对此实施单位的代表要作出承诺。

10.5.10. 产品及系统移交

文档应在申请验收时提交，系统也已上线运行，此时的移交应是一些收尾工作，

如：实施单位不应再保留正式系统的账号，以及数据的管理职能等。

10.6. 验收要求及标准

项目建设完成后，由粤澳深度合作区商事服务局提出验收申请。商事服务局牵头组织相关部门，依据项目的合同或招投标文件内容对完工项目进行验收。

（1）项目验收应当遵循“整体立项，整体验收”的原则，所有建设内容全部完成后，方可申请验收。确需分阶段验收项目，应报经商事服务局核准。

（2）为推动政府信息资源优化配置和有效利用，促进政府信息共享，对于未按照建设方案的要求实现信息共享的信息化项目不予验收。

（3）如达不到验收要求，商事服务局以书面形式通知项目承建单位，限期整改，整改后横琴粤澳深度合作区商事服务局重新申请验收。

（4）应用软件系统建设需经中国合格评定国家认可委员会认可的第三方软件检测机构进行相应的验收测试。检测结果是项目验收时的重要依据。项目建设单位必须根据政府采购的有关规定选定有资质的检测单位。

（5）项目须按照《信息安全等级保护管理办法》、《广东省计算机信息系统安全保护条例》的要求，确定信息系统的安全保护等级，二级以上信息系统须聘请第三方测评机构开展等级测评，测评合格后出具测评报告并向公安机关备案。项目建设单位必须根据政府采购的有关规定选用有资质的测评单位。

（6）项目验收过程出具的第三方检测报告、软硬件费用清单等，须具备真实性和合法性，符合国家相关法律法规和行业管理规范等。

10.6.1. 文档验收要求

文档验收标准一般包括：文档完备性、内容针对性、内容充分性、内容一致性、文字明确性、图表详实性、易读性、文档价值等。

本项目中验收评审资料包括但不限于以下部分：

基础资料：招标书、投标书、有关合同、有关批复文件、系统设计说明书、系统功能说明书、系统结构图、项目详细实施方案。

项目竣工资料：项目开工报告、项目实施报告、测试报告、操作使用说明书、售

后服务保证文件、培训文档、其他文件。

软件开发文档：需求说明书、概要设计说明书、详细设计说明书、测试计划、测试报告、用户操作手册。

软件开发管理文档：用户培训计划、质量总结报告、会议记录。

10.6.2. 质量保障体系

在本项目中，对于规划设计工作的每个关键环节和所产生的成果，制定分析和评估计划、分析和设计计划、风险管理计划和验证改进计划，采取规范的工作方法和科学的管理制度，实现本项目的质量目标。

10.6.3. 系统的验收指标要求

系统需具备 7*24 小时连续服务的能力。在连续正常负荷运行过程中，系统不会出现响应性能和响应能力下降、资源占用显著增加等现象。系统的性能指标应满足以下要求：

1、支持同时在线 400 用户，正常 20 个并发用户的性能要求；

2、响应指标，用户登录系统响应时间在 3 秒内，一般 Web 页面调用的响应时间 3 秒以内；

3、服务器内存平均占用率小于 50%，最大并发时小于 75%;

4、系统支持 7×24 小时运行。

10.6.4. 全过程质量管理

本项目实施对全过程的质量管理，把整个质量管理全过程划分为计划、实施、检查、总结处理四个阶段。四个阶段的工作完整统一，环环相扣，阶梯上升，循序渐进。