黑龙江省辰光启瑞互联网科技有限公司
印章管理审批系统 1.0 产品介绍

目录

一、前言

印章作为组织开展对外法律行为、确认内部业务效力的核心凭证，其管理规范程度直接关系到组织的合法权益与运营风险。在传统印章管理模式中，全程依赖纸质申请单流转、人工签字审批、物理印章保管的运作方式，长期面临着诸多难以解决的痛点：审批流程缺乏标准化规范，存在跨部门流转时职责划分模糊、审批节点遗漏或重复审批等问题；用章申请的发起、审批、盖章、归档等各环节缺乏完整的电子痕迹，一旦出现法律纠纷或内部审计需求，难以快速追溯业务源头与责任主体；纸质档案的

存储占用大量物理空间，且检索效率低下，跨年度、跨部门的用章记录查询往往需要耗费大量人力物力；人工操作过程中易出现申请材料丢失、审批意见填写不规范、印章使用授权边界模糊等问题，直接增加了印章滥用、越权用章的法律风险。

为彻底解决传统印章管理模式的弊端，提升印章使用与管理的规范性、可控性和可追溯性，满足组织数字化转型过程中对印章管理的精细化需求，特开发印章审批系统V1.0版本（以下简称“系统”)。本系统以“审批流程数字化、用章管理规范化、业务操作可追溯、数据存储安全化”为核心目标，构建了以审批为核心的全流程数字化用章管理基础能力，为组织提供从用章申请发起、多节点审批流转、线下盖章执行到电子档案归档的全闭环管理解决方案。

在系统设计与开发过程中，始终坚守四大核心原则：安全优先原则，将数据安全与印章使用安全贯穿于系统架构设计、功能开发、部署实施的全流程，从技术层面防范各类安全风险；最小权限原则，基于组织架构与业务需求合理划分用户角色与操作权限，确保用户仅能访问与自身职责相关的功能模块和数据资源，杜绝越权操作；可审计原则，对系统内所有关键操作进行全程日志记录，形成完整的操作审计链，满足内部审计与外部监管要求；可追溯原则，通过唯一审批编号关联用章申请、审批记录、

盖章文件、归档信息等全流程数据，实现每一次用章行为都可精准追溯源头。

为保障系统上线初期的稳定性与安全性，系统V1.0版本明确界定了功能边界，聚焦核心业务场景，剔除了高风险公开功能模块。在账号管理方面，采用“集中管控”模式，所有系统账号均由管理端统一创建、分配与维护，前端用户界面不提供任何形式的自助注册入口，从源头确保账号体系的安全性与规范性。在功能启用方面，基于风险控制与需求优先级考量，本版本暂不启用邮件发送、图形验证码、文件下载、在线预览及自动生成PDF等非核心功能，后续可根据业务发展与安全评估结果逐步扩展。在数据存储方面，系统所有业务数据、操作日志、上传文件等均存储于部署单位可控的本地服务器环境中，完全符合数据本地化管理要求与内部审计规范，确保数据资产的自主管控与安全保密。

本系统的推出，旨在为组织构建一个安全、高效、规范的数字化印章管理平台，通过技术手段将印章管理从传统人工模式升级为标准化、流程化、可追溯的数字化管理模式，有效降低用章风险，提升管理效率，为组织的合规运营与数字化转型提供坚实支撑。

二、功能介绍

本章节基于系统V1.0版本的实际开发实现，全面、详细地阐述系统核心功能模块与操作流程，所有功能描述均为已落地的实际功能，不包含未实现、已删除或规划中的功能。为确保文档表述的统一性与准确性，系统相关操作主体统一命名为：用户端（发起用章申请的操作主体）、审批端（处理用章申请的操作主体）、管理端（负责系统配置、账号管理、权限分配的操作主体）、盖章端（执行线下盖章操作并上传盖章文件的操作主体）。

2.1 账号体系与权限管理

账号体系与权限管理是保障系统安全有序运行的核心基础，系统采用“集中创建、分级授权、动态管控”的账号权限管理模式，确保每一位用户的操作行为都在授权范围内进行。

2.1.1 账号创建与维护

系统所有账号均由管理端管理员统一创建与维护，管理员登录管理端后，进入“用户管理”模块，可执行账号创建、信息编辑、状态管控等操作。在创建账号时，管理员需录入完整的用户基础信息，包括用户名（系统内唯一标识，支持字母、数字组合，长度为6-20位）、所属部门（从预设的部门架构中选择，支持多级

部门关联)、分配角色（关联系统预设的角色模板或自定义角色)、设置初始密码（默认密码需符合系统密码策略，由管理员统一配置并告知用户)。

对于已创建的账号，管理端支持实时编辑用户信息，包括更新用户昵称、调整所属部门、变更关联角色、重置登录密码等操作。同时，管理员可根据用户在职状态（如离职、调岗）灵活控制账号状态，执行启用或禁用操作：账号启用时，用户可正常登录系统并执行授权操作；账号禁用后，用户无法登录系统，且所有关联的未完成操作（如待提交的申请、待处理的审批）将被冻结，确保离职人员无法继续使用系统资源，避免信息泄露或误操作风险。

为满足审计与追溯需求，系统自动记录每一位用户的历史登录记录，管理端可通过“登录日志查询”模块，按用户名、时间范围、登录状态等条件检索用户登录信息，登录记录包含用户名、登录时间（精确到秒)、登录 IP 地址、登录设备型号、操作系统版本、浏览器类型、登录结果（成功/失败）等详细字段，便于管理员监控账号使用情况，及时发现异常登录行为。

2.1.2 密码管理策略

为保障账号登录安全，系统内置严格的密码管理机制，用户首次登录系统时，系统将强制引导用户修改初始密码，初始密码修改完成后才能进入系统主界面。密码设置需遵循系统预设的密码策略，具体要求包括：密码长度不少于 12 位；必须包含大写字母、小写字母、数字及特殊符号（支持!@#$%^&*等常见符号）四种字符类型；不得使用与用户名、手机号、邮箱相关的连续性字符或重复字符；不得使用前三次使用过的历史密码。

系统支持管理端配置周期性密码更换策略，管理员可在“系统设置-安全配置”模块中设置密码有效期（如 90 天），密码有效期届满前 7 天，系统将通过登录弹窗、首页通知等方式提醒用户及时修改密码；若用户未在有效期内完成密码修改，账号将自动锁定，需联系管理员重置密码后才能解锁使用。

同时，系统设置登录失败锁定机制，管理员可配置登录失败阈值（默认 5 次），当用户连续输入错误密码达到阈值时，账号将自动锁定，锁定时长可由管理员配置（默认 30 分钟），锁定期间不允许再次尝试登录。账号锁定事件将被实时记录到系统日志中，包含锁定账号、锁定时间、锁定原因、尝试登录的 IP 地址等信息，管理员可通过管理端查看锁定记录，并根据实际情况执行手动解锁操作。

2.1.3 基于角色的访问控制（RBAC）模型

系统采用行业成熟的基于角色的访问控制（RBAC）模型，实现权限的精细化分配与高效管理。权限管理分为三个层级：权限项、角色、用户，权限项是系统操作的最小单位（如“提交用章申请”“审批用章申请”“导出操作日志”等），角色是若干权限项的集合，用户通过关联角色获得对应的操作权限。

管理端支持两种角色配置方式：预设角色模板与自定义角色。系统预设四类基础角色模板，分别为：普通用户（仅拥有用章申请提交、申请状态查询、盖章文件上传等基础权限）、审批员（拥有待办审批查看、审批处理、审批记录查询等权限）、盖章员（拥有待盖章申请查看、盖章文件上传、盖章记录查询等权限）、系统管理员（拥有账号管理、权限配置、系统设置、日志导出等全部权限）。

管理员可根据组织实际业务需求，在预设角色模板的基础上进行修改，或创建全新的自定义角色。创建自定义角色时，管理员需为角色命名（如“法务审批员”“部门管理员”）、设置角色描述，然后从系统权限清单中勾选该角色所需的权限项，权限项覆盖系统所有操作模块，包括账号管理、申请管理、审批管理、文件管理、日志管理、系统配置等，支持按模块批量勾选或精准选

择单个权限项。

角色创建完成后，管理员可将角色批量分配给多个用户，或为单个用户分配多个角色，用户的最终权限为所分配所有角色权限项的集合。当组织业务流程或岗位职责发生变化时，管理员可通过修改角色权限项或调整用户关联角色的方式，实现权限的快速变更，权限变更操作将实时生效，并记录到系统管理日志中，包含变更人、变更时间、变更前权限、变更后权限、变更原因等信息，确保权限调整的可追溯性。

2.2 登录功能

登录功能是用户进入系统的唯一入口，系统采用“账号密码校验+安全日志记录”的登录机制，确保登录过程的安全性与可追溯性，同时为未来功能扩展预留技术接口。

2.2.1 登录流程与校验机制

用户需通过系统指定的登录页面进入系统，登录页面仅提供用户名、密码输入框及“登录”“忘记密码”两个操作按钮，不设置任何自助注册入口，所有账号均需由管理端统一创建。用户输入用户名和密码后，点击“登录”按钮，系统后端将执行一系列校

验流程：首先校验用户名是否存在于系统数据库中，若用户名不存在，返回“账号不存在，请联系管理员”的提示；若用户名存在，校验账号状态是否为“启用”，若账号处于禁用或锁定状态，返回“账号已禁用/锁定，请联系管理员”的提示；最后校验输入的密码与数据库中存储的密码哈希值是否一致，若密码不一致，返回“密码错误，请重新输入”的提示，并记录登录失败次数。

校验通过后，系统后端将生成唯一的会话标识（Session ID），会话标识采用随机字符串生成，长度为 32 位，与用户账号、登录 IP、登录设备信息绑定，有效期可由管理员在管理端配置（默认 2 小时）。系统将会话标识存储在服务器端，并通过 Cookie 将会话标识发送至用户客户端，后续用户在系统内执行的所有操作，均需通过会话标识进行身份验证，确保操作请求的合法性。

用户登录成功后，系统将自动记录登录日志，日志信息包含用户名、登录时间（精确到毫秒）、登录 IP 地址（支持 IPv4 和 IPv6 格式）、登录设备型号、操作系统版本、浏览器类型及版本、登录地点（根据 IP 地址解析的省/市/区信息）、登录结果（成功）等字段，为后续审计提供完整依据。

2.2.2 预留功能模块说明

为满足未来业务扩展需求，系统在代码层面预留了图形验证码模块接口，但在V1.0版本中，前端界面隐藏验证码输入入口，不向用户开放验证码功能。图形验证码模块采用基于AI的干扰码生成技术，支持动态生成包含数字、字母、汉字的随机验证码图片，具备扭曲、叠加、噪点等干扰效果，可有效防范暴力破解、自动化脚本攻击等风险。该模块的接口已完成标准化设计，并在代码中添加详细注释，后续可根据安全需求评估结果，快速启用该功能，启用时仅需在管理端进行配置，无需修改核心代码架构。

2.2.3 登录传输安全建议

为保障登录过程中账号密码等敏感信息的传输安全，建议在生产环境部署时启用HTTPS协议。HTTPS协议采用SSL/TLS加密技术，对客户端与服务器之间的所有数据传输进行加密处理，防止数据在传输过程中被窃取、篡改或伪造。系统支持主流的TLS 1.2及以上版本加密协议，管理员在部署时需配置合法的SSL证书（建议从权威CA机构申请），并在Web服务器（如Nginx、Apache）中进行HTTPS相关配置，确保登录页面及系统所有页面均通过HTTPS协议访问，进一步提升系统登录安全等级。

2.3 用章申请提交

用章申请提交是用户端的核心功能，系统通过标准化的申请流程、规范化的表单设计、严格的数据校验，确保用章申请信息的完整性与准确性，为后续审批环节提供可靠依据。

2.3.1 申请流程与表单设计

拥有用章申请提交权限的用户，登录用户端后，系统首页将展示“发起用章申请”快捷入口，点击后进入申请提交页面。申请提交页面采用分步引导式设计，分为“基本信息填写”“申请材料上传”“申请信息确认”三个步骤，用户需按顺序完成各步骤操作后才能提交申请。

在“基本信息填写”步骤，用户需填写标准化的申请表单，表单字段根据组织用章管理规范配置，分为必填字段和可选字段：

• 必填字段包括：申请标题（需明确说明用章用途，长度为 10-50 字，如“XX 项目合作协议盖章申请”）、用章用途（从预设选项中选择，包括合同签署、公文用印、合作协议、证明文件、其他等，可由管理端自定义配置选项）、文件类型（支持选择单一

类型或多种类型组合，如 Word 文档、PDF 文件、图片、Excel 表格等）、所属部门（默认显示用户所属部门，支持下拉选择修改，需与申请业务所属部门一致）、申请说明（详细描述用章背景、用章文件数量、是否紧急等信息，长度不少于 50 字）、申请人联系方式（手机号，需符合 11 位手机号码格式，用于紧急事项沟通）；

• 可选字段包括：紧急程度（默认普通，支持选择紧急、特急，紧急申请将在审批端待办列表中优先显示）、预计用章时间（选择具体日期，便于盖章端提前安排用章计划）、备注信息（填写其他需要说明的特殊事项）。

表单填写过程中，系统实时进行字段校验，对于必填字段，若用户未填写，将在字段下方显示红色提示信息，且无法进入下一步操作；对于格式要求严格的字段（如手机号），若用户输入不符合规范，系统将即时提示错误并引导修正。

2.3.2 申请材料上传与管理

完成基本信息填写后，进入“申请材料上传”步骤。系统支持常见的图片与文档格式文件上传，包括 JPG、PNG、GIF、BMP 等图片格式，以及 Word（doc、docx）、Excel（xls、xlsx）、PDF、

TXT 等文档格式，单个文件大小限制可由管理端配置（默认不超过 200MB），单次申请支持上传多个文件（默认最多 10 个，可配置调整）。

用户可通过两种方式上传文件：点击上传区域选择本地文件，或直接将本地文件拖拽至上传区域。文件上传过程中，系统将显示上传进度条，实时展示上传百分比，上传完成后，页面将显示文件名称、文件类型、文件大小、上传时间等信息，并支持文件预览（仅显示文件基本信息，不支持内容预览）、删除、替换等操作。若用户需上传多个文件，可重复上传操作，系统将自动对上传文件进行排序编号。

为确保上传文件的完整性与可追溯性，系统将记录每一份上传文件的元数据信息，并存储至数据库中，元数据字段包括：文件 ID（系统自动生成的唯一标识）、文件路径（存储在本地服务器的绝对路径，采用加密命名方式，避免路径泄露）、上传人（关联申请人账号）、上传时间（精确到毫秒）、文件类型（详细格式说明）、文件大小（以字节为单位）、文件哈希值（采用 MD5 算法计算的唯一校验码，用于验证文件完整性）、文件状态（正常、已替换、已删除）等。

2.3.3 申请提交与状态流转

完成申请材料上传后，进入“申请信息确认”步骤，页面将汇总展示用户填写的所有基本信息和上传的文件列表，用户需仔细核对信息是否准确。若发现错误，可点击“返回修改”按钮回到对应步骤进行修正；若信息无误，点击“提交申请”按钮，系统将执行最终的数据校验，包括必填字段完整性校验、文件上传状态校验、业务规则校验（如所属部门与申请人权限匹配校验）等，校验通过后，申请将正式提交，系统自动记录申请提交时间（精确到毫秒）和提交设备信息（包括设备型号、IP 地址、操作系统等），并将申请状态更新为“待审批”。

申请提交后，用户可在用户端“我的申请”模块中查看申请状态，包括待审批、审批中、已通过、已驳回、待盖章、已归档等状态，并可查看申请的详细信息、审批记录、文件信息等。若申请处于“待审批”状态，且审批端尚未开始处理，用户可执行撤回申请操作，撤回后可修改申请信息并重新提交；若审批端已开始处理，用户无法撤回申请，需联系审批人沟通处理。

2.4 审批管理

审批管理是系统的核心业务流程之一，系统通过标准化的审批流转机制、清晰的权限划分、完整的记录留存，确保审批过程的规

范、高效与可追溯。依托分级审批、权责对应的设计原则，结合串行、并行、会签等灵活的审批模式，适配不同业务场景下的用章审批需求，既保障审批质量，又提升审批效率。

2.4.1 审批任务接收与展示

审批端用户登录系统后，首页将展示“待办审批”模块，作为审批任务的核心入口，实时推送待处理的用章申请任务，确保审批人不会遗漏关键事项。待办审批列表采用卡片式布局，每张卡片清晰展示单条申请的核心信息，包括申请编号（系统自动生成的唯一标识，格式为“YZ-年份-月份-序号”，如“YZ-2024-10-0001”）、申请标题、发起人姓名及所属部门、发起时间、用章用途、紧急程度（通过红色“特急”、橙色“紧急”、灰色“普通”标签区分）、当前审批节点等关键字段，方便审批人快速筛选优先级任务。

为提升审批效率，待办列表支持多维度筛选与排序功能。筛选条件包括：所属部门（支持多选，可快速筛选特定部门的申请）、用章用途（按系统预设的合同签署、公文用印、证明文件等分类筛选）、紧急程度（普通/紧急/特急）、申请时间范围（今日/昨日/近 7 天/近 30 天/自定义日期）、申请状态（待审批/审批中）；排序方式支持按发起时间（升序/降序）、紧急程度（降

序，特急优先）、审批节点（升序，按流程顺序排列），审批人可根据工作习惯灵活配置展示顺序。

除首页待办模块外，审批端还设有“审批管理”专属菜单，包含待办审批、已办审批、我的审批、抄送我的四个子模块，实现审批任务的分类管理。其中：“待办审批”仅展示当前需本人处理的未完成申请；“已办审批”记录所有本人已处理（通过/驳回/加签）的申请，支持按相同筛选条件查询历史记录；“我的审批”展示由本人发起的所有用章申请的审批进度；“抄送我的”展示其他审批流程中抄送过来的申请，仅提供查看权限，无需操作处理。

为确保审批任务及时处理，系统内置多重提醒机制。当有新的审批任务推送时，系统将触发即时通知：PC 端通过右下角弹窗提醒（显示申请标题、发起人、发起时间，点击可直接跳转至审批页面）；移动端（若已部署）通过推送消息提醒；同时，系统首页待办审批模块将显示未处理任务数量红点，直观提示待办事项。对于超时未处理的审批任务，系统将自动触发二次提醒：管理员可在管理端设置超时阈值（默认 24 小时），当审批任务超出阈值未处理时，系统将向审批人发送超时提醒（支持配置为系统内通知或短信提醒），同时同步至审批人的直接上级，确保流程不卡顿。

审批人点击待办列表中的任意申请卡片，将进入审批详情页面。该页面采用分区域展示设计：左侧为申请信息区，完整呈现申请人填写的所有基本信息（申请标题、用章用途、所属部门、申请说明、联系方式、紧急程度等）；中间为文件预览区，展示申请人上传的所有附件文件，支持查看文件名称、大小、上传时间，点击可打开文件查看内容（仅支持查看，不支持下载与编辑）；右侧为审批操作区，包含审批意见输入框、审批操作按钮（通过/驳回/加签/回退）、审批记录追溯栏（展示该申请此前所有审批节点的处理人、处理时间、审批意见），实现“信息查看-文件核验-审批操作”的一站式处理。

2.4.2 审批流程与权限配置

系统基于组织架构与业务需求，采用可视化流程建模设计，支持灵活配置审批流程，满足不同用章场景的分级审批需求。审批流程的配置由管理端管理员统一操作，管理员进入“流程配置”模块后，可通过拖拽式操作搭建审批节点，定义流转规则，无需代码开发，实现快速适配业务变化。

审批流程支持按用章类型、文件重要程度、申请部门等条件设置分支流转规则。例如：普通证明文件用章申请，流程为“申请人

发起→部门主管审批→盖章端执行”；金额较大的合同用章申请，流程为“申请人发起→部门主管初审→法务部合规审核→分管领导审批→总经理终审→盖章端执行”；跨部门用章申请，流程为“申请人发起→本部门主管审批→协作部门确认→分管领导审批→盖章端执行”￼。管理员可根据组织实际制度，自定义配置分支条件与对应审批节点，确保审批流程与管理规范高度契合。

系统支持多种审批模式，适配不同场景的决策需求：

• 串行审批：流程按预设节点依次流转，前一节点审批通过后，才能进入下一节点，适用于需严格层级把关的场景（如大额合同用章、涉及公司重大权益的文件用章），确保每一层级都能充分审核；

• 并行审批：多个审批节点同时接收审批任务，可独立处理，全部通过后流程继续流转，适用于需多部门同步确认的场景（如项目立项相关文件用章，需业务部、财务部、法务部同时审核），缩短审批周期；

• 会签审批：指定多名审批人共同审批，需所有审批人全部同意方可通过，适用于重要决策类用章场景（如“三重一大”事项相

关文件用章），确保决策合规；

• 加签/回退审批：审批人在处理任务时，可根据实际需求临时添加其他审批人（加签，支持指定具体人员或角色），或将流程退回至前一审批节点（回退，需填写退回原因），应对审批过程中的特殊情况，提升流程灵活性OBJOBJOBJ。

审批权限的分配严格遵循“最小权限原则”与“权责对应原则”，基于 RBAC 模型实现精细化管控。管理员在配置审批流程时，可为每个审批节点指定具体的审批人或审批角色：指定具体人员时，流程将直接推送至该用户；指定角色时，流程将推送至该角色下的所有用户（支持配置为“任意一人审批通过即可”或“所有人员审批通过方可”）。例如：法务部审核节点指定“法务专员”角色，流程将推送至所有法务专员，配置为“任意一人审批通过即可”，提升审批效率；总经理终审节点指定“总经理”具体人员，确保核心决策由指定负责人把控。

为避免审批人因离职、调岗导致流程停滞，系统支持配置审批人替代规则。管理员可在“权限配置”模块中，为每个审批角色或具体审批人设置替代人及替代生效条件（如离职、请假、出差）。当审批人触发生效条件时，其待办审批任务将自动流转至替代人，确保审批流程持续推进，不影响业务开展。替代规则可

配置为临时替代（设置生效时间段）或永久替代，且所有替代操作均记录在系统日志中，便于追溯与审计。

2.4.3 审批操作与意见记录

审批人在审批详情页面完成信息核验与文件查看后，可执行相应的审批操作。所有审批操作均需填写审批意见，系统强制要求审批意见需明确表达审核结论（支持配置为“必填”，字数不少于10字），避免无理由审批，确保审批过程的严肃性与可追溯性。

- 审批通过操作：审批人确认申请信息真实、文件内容合规后，在意见输入框填写通过意见（如“经审核，申请材料完整，文件内容合规，同意用章”），点击“通过”按钮。系统将自动记录审批人、审批时间（精确到毫秒）、审批意见，同时根据预设流程规则，将申请流转至下一审批节点（若为最后一个审批节点，则流转至“待盖章”状态，并通知盖章端用户）。

- 审批驳回操作：若申请信息不完整、文件内容不合规或存在其他异议，审批人在意见输入框中明确填写驳回原因及修改要求（如“申请说明未明确用章文件的具体用途，缺少项目编号，建议补充后重新提交”），点击“驳回”按钮。系统将记录驳回信息，同时向申请人发送驳回通知，告知修改方向。申请人收到通

知后，可在“我的申请”模块中查看驳回意见，修改完善后重新提交申请，流程重新启动。

• 加签操作：审批人认为需其他人员协助审核时，可点击“加签”按钮，选择需加签的用户或角色，填写加签说明（如“该合同涉及涉外条款，需法务部张三专员补充审核”），点击确认。系统将该申请临时推送至加签人，加签人审核通过后，流程返回原审批节点，再由原审批人继续处理；加签人驳回时，流程直接驳回至申请人。

• 回退操作：审批人发现前一节点审批存在遗漏或错误时，可点击“回退”按钮，选择需回退的节点，填写回退原因（如“前一节点未核验文件的法律效力，建议重新审核”），点击确认。系统将申请回退至指定节点，该节点的审批人需重新处理，处理完成后再按流程流转。

系统支持审批意见的格式标准化配置，管理员可在管理端设置审批意见模板（如“经审核，申请材料完整，文件合规，同意用章”“申请信息不全，缺少 XX 材料，驳回修改”），审批人可直接选用模板并补充个性化说明，提升审批效率的同时，确保意见表述规范。所有审批记录（包括审批人、审批时间、审批意见、操作类型）均被系统永久存储，不可篡改，形成完整的审批追溯

链，供后续审计与纠纷追溯使用。

对于紧急程度为“特急”的申请，系统将自动优化审批流程：在审批端待办列表中置顶展示，同时缩短超时提醒阈值（默认 12 小时），若审批人在 1 小时内未处理，系统将自动向其上级发送督办通知，确保紧急事项快速响应。

2.4.4 审批状态跟踪与异常处理

系统为申请人、审批人、管理员提供全流程审批状态跟踪功能，不同角色可通过对应端口实时查看申请进度，确保信息透明。申请人登录用户端后，在“我的申请”模块中，可查看每笔申请的当前状态（待审批/审批中/已通过/已驳回/待盖章/已归档），点击任意申请可查看完整的审批流转记录，包括各节点的处理人、处理时间、审批意见，清晰掌握申请所处阶段。

审批人在“已办审批”模块中，可查看自己处理过的所有申请的后续流转状态，若发现流程卡在某一节点，可通过系统内沟通功能提醒对应审批人处理。管理员在管理端“流程监控”模块中，可查看所有申请的实时流转状态，支持按流程名称、申请状态、时间范围等条件筛选，直观展示流程拥堵节点（如某一审批节点平均处理时长过长），为优化审批流程提供数据支撑。

系统针对审批过程中可能出现的异常情况，提供完善的处理机制：

• 审批人离职未处理：若审批人离职后，其名下仍有未处理的审批任务，管理员可通过管理端“流程干预”模块，将该任务手动转移至替代人或其他指定审批人，同时更新审批记录，确保流程持续推进；

• 申请信息错误需修改：若审批人已通过某节点，但后续发现申请信息存在错误，可通过“回退”操作将流程退回至申请人，申请人修改后重新提交，系统将保留原审批记录，新增修改后的流转记录；

• 流程配置错误导致卡顿：若因审批流程配置错误（如缺少后续节点、分支条件冲突）导致申请无法流转，管理员可在管理端实时修改流程配置，修改后系统将自动触发流程继续流转，同时记录配置修改日志；

• 恶意提交重复申请：管理员可在管理端设置重复申请判定规则（如同一申请人在 24 小时内提交相同标题、相同文件的用章申请），系统将自动识别并拦截重复申请，或提示管理员人工审

核，避免资源占用。

所有异常处理操作均需记录在系统日志中，包含操作人、操作时间、异常原因、处理方式等信息，确保异常处理的可追溯性。同时，系统支持生成审批异常统计报表，管理员可定期查看异常类型、发生频率、处理时长等数据，针对性优化审批流程与管理规范，提升流程稳定性。

2.5 盖章管理

盖章管理是用章流程的执行环节，系统通过“线上审批确认-线下盖章执行-线上记录归档”的闭环设计，确保盖章操作的规范性与可追溯性，实现“审批有依据、盖章有记录、归档有凭证”。

2.5.1 盖章任务接收与确认

盖章端用户（印章保管人）登录系统后，首页将展示“待盖章任务”模块，实时接收经审批通过的用章申请。待盖章任务列表的展示形式与审批端待办列表一致，采用卡片式布局，每张卡片展示核心信息：申请编号、申请标题、发起人、所属部门、审批通过时间、预计用章时间、需盖章文件数量，方便盖章人快速了解

任务详情。

待盖章列表支持筛选与排序功能：筛选条件包括所属部门、用章用途、申请时间范围、任务状态（待盖章/已完成/已驳回）；排序方式支持按审批通过时间（降序，优先处理最新通过的申请）、预计用章时间（升序，优先处理紧急用章需求）。盖章人可根据实际工作安排，灵活筛选任务优先级。

盖章人点击任务卡片进入盖章详情页面，该页面与审批详情页面结构一致，左侧展示完整申请信息与审批记录，中间展示需盖章的文件列表，右侧为盖章操作区。盖章人需先核对申请信息与审批记录，确认该申请已完成所有审批节点，且审批意见均为“通过”，再核验待盖章文件与申请说明是否一致，确保盖章操作有合法审批依据。

若盖章人发现申请信息与文件存在不一致、审批流程未完成或其他异常情况，可点击“驳回”按钮，填写驳回原因（如“待盖章文件与申请说明不符，需申请人确认”），将任务退回至申请人或最后一个审批节点，同时通知相关人员处理。若信息核对无误，盖章人点击“确认接收”按钮，将任务状态更新为“处理中”，表示已开始准备盖章操作，避免重复处理。

2.5.2 线下盖章与线上记录

盖章人确认接收任务后，需从印章保管柜中取出对应印章（系统支持关联印章信息，管理员可在管理端为每个盖章任务配置对应的印章类型，如公章、合同专用章、财务专用章等，方便盖章人快速定位印章），按照申请要求在纸质文件或电子文件上完成盖章操作。

盖章操作需遵循以下规范：

- 盖章位置：确保印章清晰、完整，盖在文件的指定位置（如合同末尾的签字盖章区、证明文件的落款处），不得覆盖文件关键内容（如文字、数字、签名）；

- 盖章数量：严格按照申请人填写的“文件数量”执行，确保每一份文件都加盖对应印章，不得多盖、少盖或漏盖；

- 印章使用：仅允许使用审批流程中指定的印章类型，不得擅自更换印章或使用未经授权的印章；

- 异常处理：若盖章过程中出现印章模糊、文件破损等情况，需及时向管理员报备，重新打印文件后再行盖章，同时记录异常情

况。

盖章完成后，盖章人需在系统中完成线上记录操作：进入盖章详情页面的操作区，填写盖章记录（包括盖章时间、盖章地点、印章使用情况），上传盖章后的文件（支持上传扫描件或电子版，要求文件清晰可辨，能完整展示印章样式）。若为多份文件盖章，需按顺序上传所有盖章后的文件，系统支持批量上传与排序。

上传完成后，盖章人点击“确认完成”按钮，系统将自动记录盖章操作的所有信息（盖章人、盖章时间、盖章文件、盖章记录），并将申请状态更新为“已盖章”，同时向申请人发送盖章完成通知，告知其可领取文件或查看电子版。

2.5.3 盖章归档与追溯

系统支持对盖章后的文件与相关记录进行自动归档，形成完整的用章档案。归档操作由系统自动执行，当盖章人确认完成盖章后，系统将申请编号作为档案唯一标识，关联存储以下信息：

- 申请阶段：申请人填写的所有基本信息、上传的原始文件；

• 审批阶段：所有审批节点的处理人、审批时间、审批意见；

• 盖章阶段：盖章人、盖章时间、盖章记录、上传的盖章后文件；

• 关联信息：印章类型、归档时间、档案存储路径。

管理员可在管理端“档案管理”模块中，按申请编号、申请人、所属部门、用章用途、归档时间等条件检索归档档案，支持查看档案详情、下载归档文件（仅管理员有权限配置下载权限）、导出归档报表。归档档案将永久存储在本地服务器中，存储期限遵循组织档案管理制度（默认永久保存），满足后续审计、查询、纠纷追溯等需求。

系统支持生成盖章统计报表，管理员可查看指定时间段内的盖章总量、各印章类型使用频次、各部门用章量、盖章平均处理时长等数据，为印章管理优化提供数据支撑。例如：通过报表发现某一部门用章频率过高，可分析是否存在流程冗余；发现某类印章长期未使用，可评估是否需要调整印章保管方式。

2.6 查询与统计功能

系统提供多维度的查询与统计功能，满足用户、管理员对用章申请、审批记录、盖章记录、系统操作等数据的检索与分析需求，实现“数据可查、趋势可判、管理可控”。

2.6.1 多维度查询功能

不同角色的用户拥有对应的查询权限，确保数据访问的安全性与针对性：

- 用户端查询权限：普通用户仅能查询自己发起的所有用章申请，支持按申请状态（待审批/审批中/已通过/已驳回/待盖章/已归档）、申请时间范围、用章用途等条件筛选，查看申请详情、审批记录、盖章状态，满足个人用章记录追溯需求；

- 审批端查询权限：审批人可查询自己处理过的所有审批任务，支持按审批结果（通过/驳回/加签/回退）、处理时间范围、所属部门、用章用途等条件筛选，查看审批详情、后续流转状态，方便工作复盘与追溯；

- 盖章端查询权限：盖章人可查询自己处理过的所有盖章任务，支持按处理状态（待盖章/已完成/已驳回）、处理时间范围、所属部门等条件筛选，查看盖章详情、归档记录；

• 管理端查询权限：管理员拥有全量数据查询权限，可查询系统内所有申请、审批、盖章、账号、日志等数据，支持按任意字段组合筛选（如申请人+审批人+用章类型+时间范围），满足全局监管与审计需求。

查询功能支持精确查询与模糊查询：精确查询适用于申请编号、用户名、所属部门等固定字段；模糊查询适用于申请标题、申请说明、审批意见等文本字段，提升查询灵活性。查询结果支持导出操作（管理员可配置导出权限），支持导出为 Excel 或 CSV 格式，方便离线分析与存档。

2.6.2 统计分析与报表生成

管理端内置统计分析模块，系统自动采集用章全流程数据，生成多维度统计报表，支持可视化展示（柱状图、饼图、折线图），直观呈现用章管理情况。

核心统计报表包括：

• 用章总量统计：按时间维度（日/周/月/年）统计系统内所有用章申请的发起量、审批通过量、盖章完成量、驳回量，展示用

章业务的整体趋势；

• 部门用章统计：按部门维度统计各部门的用章申请量、审批通过率、平均审批时长、平均盖章时长，分析各部门用章需求与效率；

• 审批效率统计：按审批节点维度统计各审批人的处理量、平均处理时长、超时处理次数、驳回率，评估审批人工作效率与审批质量；

• 印章使用统计：按印章类型维度统计各印章的使用次数、对应业务类型、使用部门分布，优化印章保管与调配方案；

• 异常情况统计：统计审批驳回、盖章驳回、流程超时、重复申请等异常事项的数量、类型分布、处理结果，为管理优化提供依据。

管理员可自定义统计报表的时间范围、展示维度、筛选条件，支持将常用报表保存为模板，定期自动生成并推送至指定邮箱（需管理员配置）。同时，报表支持导出与打印功能，管理员可将报表用于内部审计、管理层汇报，为印章管理决策提供数据支撑。

2.7 日志管理

日志管理是系统安全与合规的重要保障，系统对所有关键操作进行全程记录，形成完整的操作日志链，确保每一次系统行为都可追溯、可审计，满足内部监管与外部合规要求。

2.7.1 日志类型与记录内容

系统日志涵盖五大类核心操作，每类日志均记录详细的操作信息，确保追溯的完整性：

• 登录日志：记录所有用户的登录行为，包括用户名、登录时间(精确到毫秒)、登录 IP 地址、登录设备型号、操作系统版本、浏览器类型、登录结果（成功/失败)、失败原因（账号不存在/密码错误/账号禁用/锁定)，用于监控账号安全，防范异常登录；

• 申请日志：记录用章申请的全生命周期操作，包括申请发起、修改、提交、撤回、驳回后重新提交等行为，记录字段包括申请编号、操作人、操作时间、操作类型、操作内容（如修改后的申请信息、撤回原因)，确保申请过程可追溯；

• 审批日志：记录所有审批操作，包括审批接收、通过、驳回、加签、回退等行为，记录字段包括申请编号、审批人、审批时间、审批意见、操作类型、流转节点变化，形成完整的审批追溯链；

• 盖章日志：记录盖章操作的全流程，包括盖章任务接收、确认、驳回、完成、归档等行为，记录字段包括申请编号、盖章人、操作时间、操作类型、盖章记录、上传文件名称，确保盖章操作可追溯；

• 系统管理日志：记录管理端的所有配置操作，包括账号创建、修改、禁用、密码重置、角色配置、权限调整、流程配置、系统参数设置等，记录字段包括操作人、操作时间、操作类型、操作内容（修改前/修改后参数）、操作 IP 地址，确保系统配置变更可追溯。

所有日志字段均为必填项，系统强制记录，不可遗漏。日志数据采用加密存储方式，存储在本地服务器的日志数据库中，仅管理员有权限查看与导出，确保日志数据的安全性与完整性。

2.7.2 日志查询与导出

管理员登录管理端后，进入“日志管理”模块，可按日志类型、操作人、操作时间范围、关键字段（如申请编号、用户名、IP地址）等条件筛选日志。支持精确查询与模糊查询结合，例如：筛选“2024年10月1日-2024年10月31日”期间“审批驳回”类型的日志，或模糊查询“IP地址包含192.168.1.”的登录日志。

查询结果以列表形式展示，支持按操作时间升序/降序排序，列表中展示核心日志字段，点击任意日志条目可查看完整日志详情。日志详情页面将完整呈现该条日志的所有记录字段，确保信息不遗漏。

系统支持日志导出功能，管理员可将查询结果导出为Excel、CSV或PDF格式，导出文件包含所有日志字段，便于离线存档与审计。导出操作需记录在系统管理日志中，包括导出人、导出时间、导出日志类型、导出条件、导出文件大小，确保导出行为可追溯。

为保障日志数据的安全性，管理员可配置日志导出权限：支持设置仅指定管理员可导出日志，或导出日志时需输入二次验证密码。同时，系统支持日志备份功能，管理员可设置自动备份周期（默认每日备份），将日志数据备份至指定存储设备，防止日志丢

失。

2.7.3 日志留存与审计应用

系统日志的留存期限遵循国家相关法律法规与组织内部制度，默认留存期限为 3 年，管理员可在管理端根据实际需求调整（最长支持永久留存）。日志数据采用循环存储机制：当存储容量达到阈值时，系统将自动删除最早的日志数据（需提前备份），或提示管理员扩容存储设备，确保日志存储的连续性。

日志数据是系统审计与安全排查的核心依据，主要应用于以下场景：

- 内部审计：审计人员可通过查询日志，核实用章申请、审批、盖章流程是否符合组织制度，检查是否存在越权审批、无理由驳回、违规盖章等行为；

- 安全排查：当出现账号异常登录、数据泄露等安全事件时，管理员可通过登录日志、系统管理日志追溯异常行为的操作人、操作时间、操作 IP，定位安全风险源头；

- 纠纷处理：当用章行为引发法律纠纷时，可通过申请日志、审

批日志、盖章日志核实申请的真实性、审批的合规性、盖章的规范性，提供有力的追溯凭证；

• 责任认定：当出现用章错误、文件遗漏等问题时，可通过日志明确申请、审批、盖章各环节的责任人，为责任认定提供依据。

管理员可定期生成日志审计报表，统计日志查询频次、审计发现的问题、问题处理结果等信息，持续优化系统安全管控与用章管理规范。

2.8 系统设置

系统设置是管理端的核心功能模块，由管理员统一操作，用于配置系统参数、优化操作体验、保障系统安全稳定运行。系统设置支持灵活调整，无需修改核心代码，即可适配组织业务变化与管理需求。

2.8.1 基础参数配置

管理员进入“系统设置-基础配置”模块，可配置以下核心参数：

• 系统名称：可自定义系统显示名称（如“XX 公司印章审批系统”），配置后将在系统登录页面、首页标题栏显示；

• 组织信息：填写组织名称、所属行业、联系人、联系电话等信息，用于系统内通知、报表页眉等场景展示；

• 时间配置：设置系统时间格式（如 YYYY-MM-DD HH:MM:SS）、时区（默认北京时间）、日期默认显示方式；

• 分页设置：配置各模块列表页面的默认显示条数（如 10 条/20 条/50 条），用户可在前端根据习惯调整；

• 文件配置：设置文件上传的格式限制（如允许上传的图片、文档类型）、单个文件大小限制（默认 200MB，可调整）、单次申请上传文件数量上限（默认 10 个，可调整）；

• 通知配置：设置系统通知的发送方式（系统内弹窗/短信提醒）、提醒触发条件（如审批通过/驳回、盖章完成、超时未处理）、短信提醒的接收号码（仅管理员可配置）。

基础参数配置完成后，点击“保存”按钮即时生效，所有用户端、审批端、盖章端将同步更新配置结果。系统自动记录参数修

改日志，包括修改人、修改时间、修改前参数、修改后参数，确保配置变更可追溯。

2.8.2 安全参数配置

管理员进入“系统设置-安全配置”模块，可配置以下安全参数，强化系统安全防护：

• 密码策略：设置密码长度（默认不少于 12 位）、字符类型要求（大写字母、小写字母、数字、特殊符号）、密码有效期（默认 90 天）、历史密码限制（默认不允许使用前 3 次密码）、登录失败锁定阈值（默认 5 次）、锁定时长（默认 30 分钟）；

• 会话管理：设置用户登录后的会话有效期（默认 2 小时），会话超时后用户需重新登录；配置会话标识（Session ID）的生成规则与长度，提升会话安全性；

• IP 白名单：配置允许登录系统的 IP 地址范围，仅在白名单内的 IP 地址可访问系统，防范异地登录风险；支持添加多个 IP 段，灵活适配办公场景；

• 操作权限控制：配置敏感操作的二次验证（如账号禁用、权限

修改、流程配置变更等操作，需输入管理员二次验证密码），防止误操作；

• 数据加密配置：设置用户密码的加密算法（默认采用 SHA-256 加密）、敏感数据（如手机号、申请说明）的加密存储方式，确保数据安全。

安全参数配置直接关系到系统安全，管理员修改时需谨慎操作，修改后系统将即时生效。系统支持导出当前安全配置方案，便于备份与后续恢复。

2.8.3 流程参数配置

管理员进入“系统设置-流程配置”模块，可配置审批流程的相关参数，优化流程流转效率：

• 超时阈值：设置审批节点的超时阈值（默认 24 小时）、盖章任务的超时阈值（默认 48 小时），超时后系统自动触发提醒；

• 驳回规则：配置审批驳回后是否允许申请人重新提交（默认允许，可设置为不允许）、重新提交的次数限制（默认无限制，可设置为 3 次以内）；

• 流程跳转规则：配置审批通过后是否自动跳转至下一节点（默认自动跳转）、加签/回退操作后的流程流转规则；

• 紧急申请规则：配置紧急申请的判定条件（如申请人选择“紧急/特急”）、紧急申请的流程优先级（默认置顶展示、缩短超时阈值）。

流程参数配置完成后，将应用于所有审批流程，管理员可根据业务反馈持续优化参数，提升流程适配性。

三、产品实用性

印章审批系统 V1.0 的核心价值在于解决传统印章管理模式的痛点，通过数字化、标准化、可追溯的管理方式，提升用章管理效率、降低运营成本、防范法律风险，其实用性主要体现在场景适配、操作便捷、成本优化、风险管控四大维度。

3.1 场景适配性：覆盖全流程用章需求

系统基于组织日常用章的核心场景设计，全面覆盖内部公文用印、对外合同签署、证明文件盖章、跨部门协作用章、紧急事项

用章等各类场景，适配不同规模、不同行业组织的用章管理需求。

对于中小型组织，系统支持简化审批流程（如“申请人发起→部门主管审批→盖章执行”），满足快速用章需求；对于大型组织或层级复杂的组织，系统支持多级审批、跨部门审批、会签审批等复杂流程配置，适配精细化管理要求。例如：企业行政部门申请公文用印，流程可配置为“申请人发起→行政主管审批→盖章执行”；法务部门申请合同用印，流程可配置为“申请人发起→部门主管初审→法务合规审核→分管领导审批→总经理终审→盖章执行”，确保不同场景的用章流程均符合组织管理规范。

系统支持自定义用章用途、文件类型、审批节点等配置项，管理员可根据组织业务变化（如新增业务线、调整管理架构）灵活调整，无需二次开发，即可快速适配新的用章场景。例如：组织新增涉外业务，需新增“涉外合同用章”类型，管理员可在管理端直接添加该用章用途，并配置对应的审批流程（如增加“涉外业务部审核”节点），系统即时生效。

3.2 操作便捷性：降低用户使用门槛

系统采用“以用户为中心”的设计理念，界面布局简洁清晰，操

作流程标准化，无需专业技术知识，普通员工即可快速上手，大幅降低培训成本。

3.2.1 多端适配，随时随地操作

系统支持PC端、移动端（兼容iOS、Android系统）、平板端多终端登录，用户可根据场景灵活选择操作设备：申请人可在办公室通过PC端发起申请、上传文件；审批人外出时可通过移动端接收审批提醒、处理待办任务；盖章人在印章保管室可通过平板端查看任务、上传盖章文件。多端操作体验一致，数据实时同步，打破时空限制，提升办公效率OBJOBJOBJ。

3.2.2 流程简化，减少操作步骤

用章申请流程简化为“填写信息→上传文件→提交申请”三步，审批流程简化为“查看详情→填写意见→执行操作”三步，盖章流程简化为“核对信息→线下盖章→上传文件→确认完成”四步，每一步操作均有明确的引导提示（如必填字段标注、按钮高亮显示），避免用户操作失误。

系统支持表单字段自动填充功能：申请人填写基本信息时，所属部门、联系方式等字段默认显示当前用户的关联信息，无需手动

输入；审批人处理审批时，系统自动展示此前的审批记录，无需反复查询；盖章人处理任务时，系统自动关联对应的印章类型，方便快速定位。

3.2.3 智能提醒，减少人工跟进

系统内置多重智能提醒机制，替代传统的人工催办、跟进，减少沟通成本。例如：申请人发起申请后，系统自动提醒审批人处理；审批通过后，自动提醒盖章人执行；盖章完成后，自动提醒申请人领取文件；流程超时未处理时，自动提醒相关责任人与管理员，确保流程高效推进，无需申请人反复跟进询问。

3.3 成本优化：降低管理与运营成本

传统印章管理模式中，纸质申请单打印、传递、存储需耗费大量人力、物力、空间成本，系统通过数字化转型，从多个维度降低组织运营成本。

3.3.1 人力成本优化

无需专人负责纸质申请单的传递、分发、归档，申请人在线发起申请，审批人在线处理，盖章人在线接收任务，全流程自动化流

转，减少中间环节的人力投入。例如：传统模式下，跨部门用章申请需申请人亲自将纸质单据送至各审批部门，平均耗时 1-2 天；系统上线后，申请在线流转，各审批节点实时接收任务，平均审批时长缩短至 2-4 小时，人力成本降低 60%以上。

3.3.2 物料成本优化

彻底摒弃纸质申请单、审批表，所有申请、审批、盖章记录均以电子形式存储，减少纸张、打印耗材、笔墨等物料的消耗，符合绿色办公理念。按组织日均 10 笔用章申请计算，传统模式下年均消耗纸张约 3600 张，系统上线后可完全节省该部分物料成本，且随着用章量增加，成本节省效果更显著。

3.3.3 空间成本优化

传统模式下，纸质用章档案需占用专门的档案室存储，且存储期限长，空间占用持续增加；系统上线后，所有电子档案存储在本地服务器中，占用空间小，且支持按申请编号、时间范围等快速检索，无需专人管理档案室，节省物理空间与管理成本。例如：10 年的用章电子档案仅需占用约 50GB 存储空间，而同等数量的纸质档案需占用 10 平方米以上的档案室。

3.4 风险管控：防范用章法律风险

传统印章管理模式中，无记录、越权用章、印章滥用等行为易引发法律纠纷，系统通过全流程追溯、权限管控、合规校验等功能，从源头防范用章风险，保障组织合法权益。

3.4.1 全流程追溯，责任可认定

每一次用章行为都形成完整的追溯链：申请信息、审批记录、盖章操作、归档文件均永久存储，不可篡改，一旦出现法律纠纷，可快速调取相关记录，明确责任主体。例如：某合同用章后出现条款争议，通过系统可查询该合同的申请说明、审批意见、盖章记录，核实用章行为的合规性，为纠纷处理提供有力凭证。

3.4.2 权限管控，杜绝越权操作

基于RBAC模型的权限管理，确保“谁有权、谁操作”：普通用户仅能发起自身职责范围内的用章申请；审批人仅能处理授权范围内的审批任务；盖章人仅能使用指定印章执行盖章操作；管理员的配置操作均有日志记录，杜绝越权用章、违规审批等行为。例如：部门主管无权审批超出部门权限的大额合同用章申请，系统将自动流转至分管领导，避免越权决策风险。

3.4.3 合规校验，降低法律风险

系统支持配置合规校验规则：管理员可在管理端设置用章申请的合规条件（如合同用章需上传法务审核意见、对外承诺类文件用章需总经理审批），申请人发起申请时，系统自动校验是否符合合规条件，不符合则无法提交；审批人处理时，系统自动提示该申请需重点审核的合规要点（如是否涉及涉外条款、是否超出授权金额），降低因文件不合规引发的法律风险。

四、产品安全系数

印章审批系统 V1.0 将安全性贯穿于系统架构、功能设计、数据存储、操作流程的全流程，采用行业成熟的安全技术与管控机制，从物理安全、网络安全、数据安全、应用安全四个维度构建全方位安全防护体系，确保系统稳定运行，数据安全保密。

4.1 物理安全：保障硬件与环境安全

系统所有数据均存储于组织本地服务器，服务器部署在专用机房，具备完善的物理安全防护措施：

• 机房环境：机房采用恒温恒湿设计，温度控制在 18-24℃，湿度控制在 40%-60%，配备精密空调、ups 不间断电源，防止因环境异常导致服务器故障；

• 访问控制：机房实行 24 小时门禁管理，仅授权人员（如机房管理员、IT 负责人）可进入，进入时需进行身份验证（指纹+密码），并记录访问日志；

• 监控防护：机房安装 360 度无死角视频监控，监控录像保存期限不少于 90 天，实时监控服务器运行状态与机房环境；

• 防灾防护：机房配备消防设施（如气体灭火系统）、防雷装置，定期进行安全检测，防范火灾、雷击等自然灾害风险；

• 硬件冗余：服务器采用双机热备架构，当主服务器出现故障时，备用服务器自动切换，确保系统不间断运行，数据不丢失。

4.2 网络安全：防范网络攻击与入侵

系统采用多层次网络安全防护设计，保障网络传输与通信安全：

• 防火墙部署：在服务器与外部网络之间部署下一代防火墙

(NGFW)，配置访问控制策略，仅开放系统所需的端口（如 80 端口、443 端口），拦截非法访问、端口扫描、恶意攻击等网络威胁；

• 入侵检测与防御：部署入侵检测系统（IDS）与入侵防御系统（IPS），实时监控网络流量，识别并阻断 SQL 注入、跨站脚本（XSS）、缓冲区溢出等常见网络攻击，保护服务器安全；

• VPN 访问控制：远程用户（如外出审批人、异地管理员）需通过虚拟专用网络（VPN）接入系统，VPN 采用强加密协议（如 IPsec），确保远程访问的安全性，防止数据在传输过程中被窃取；

• 网络隔离：将系统服务器部署在内部局域网，与互联网进行逻辑隔离，仅通过指定网关进行数据交互，减少外部网络威胁攻击面；

• 网络审计：部署网络审计系统，记录所有网络访问行为（访问 IP、访问时间、访问端口、数据传输量），定期分析审计日志，及时发现异常网络行为。

4.3 数据安全：确保数据存储与传输安全

数据安全是系统安全的核心，系统采用多种加密技术与管控机制，保障数据全生命周期安全：

• 数据传输加密：系统所有数据传输均采用 HTTPS 协议加密（基于 TLS 1.2 及以上版本），对客户端与服务器之间的所有通信数据进行加密处理，防止数据在传输过程中被窃取、篡改或伪造；

• 数据存储加密：用户密码采用 SHA-256 哈希算法加密存储，数据库中不存储明文密码；敏感业务数据（如申请说明、审批意见、联系方式）采用 AES-256 加密算法存储，加密密钥由管理员专人保管，定期更换；

• 数据库安全：采用数据库审计系统，记录所有数据库操作（查询、插入、修改、删除），实时监控数据库访问行为；配置数据库备份策略（每日全量备份+增量备份），备份数据存储在异地服务器，防止数据丢失；

• 数据访问控制：基于角色的权限分配，确保用户仅能访问与自身职责相关的数据，例如普通用户无法查看其他用户的申请记录，审批人无法访问系统管理日志，防止数据泄露；

• 数据销毁：对于超出留存期限的日志数据、废弃业务数据，采用安全销毁方式（如多次覆写、物理销毁存储介质），确保数据无法被恢复，符合数据安全合规要求。

4.4 应用安全：防范应用层漏洞与风险

系统在应用层设计中融入多项安全机制，防范应用漏洞引发的安全风险：

• 输入验证：对所有用户输入的信息（如用户名、密码、申请信息、审批意见）进行严格校验，过滤非法字符、特殊符号，防止SQL 注入、XSS 攻击等漏洞利用；

• 会话安全：会话标识（Session ID）采用随机字符串生成，长度为 32 位，与用户账号、登录 IP、设备信息绑定，会话超时后自动失效；禁止通过URL 传递会话标识，防止会话劫持；

• 防重复提交：系统采用令牌（Token）机制，防止同一申请被重复提交，每次申请提交时生成唯一 Token，提交成功后 Token 失效，避免重复操作导致的数据冗余；

• 权限最小化：严格遵循权限最小化原则，仅为用户分配完成工

作所需的最小权限，例如普通用户无审批权限，审批人无账号管理权限，减少权限滥用风险；

• 安全测试：系统上线前经过全面的安全测试（包括漏洞扫描、渗透测试、代码审计），上线后定期进行安全巡检，及时修复发现的安全漏洞，持续提升应用安全等级。

4.5 安全管理：建立完善的安全管控机制

除技术层面的安全防护外，系统还通过管理制度与流程管控，构建全方位安全保障体系：

• 安全责任制：明确系统管理员、审批人、申请人、盖章人的安全职责，签订安全责任书，将安全责任落实到个人；

• 账号管理制度：建立严格的账号申请、创建、使用、变更、注销流程，员工离职后及时禁用账号，防止账号被盗用；

• 密码管理制度：要求用户定期更换密码，严禁共用账号密码、使用弱密码，管理员定期检查密码合规性，对违规密码进行强制修改；

• 安全培训：定期对系统用户进行安全培训，普及账号安全、数据安全、防范网络攻击等知识，提升用户安全意识；

• 应急响应机制：制定系统安全应急预案，明确安全事件（如数据泄露、系统入侵、服务器故障）的处理流程、责任分工、应急措施，定期组织应急演练，确保快速响应安全事件。

五、产品具体介绍

5.1 产品定位

印章审批系统 V1.0 是一款面向各类组织（企业、事业单位、政府机构等）的数字化印章管理工具，核心定位是“用章流程标准化、管理行为可追溯、安全风险可控化”。产品以解决传统印章管理的痛点为核心目标，摒弃“纸质申请、人工流转、线下存档”的传统模式，通过数字化手段构建全流程闭环管理体系，为组织提供“申请-审批-盖章-归档”一站式用章管理解决方案。

产品不局限于单一的流程审批功能，更注重用章风险的全流程管控与管理效率的提升，适用于需要规范印章使用、防范用章风险、提升管理效率的各类组织，尤其适配层级复杂、跨部门协作频繁、用章需求量大的组织。

5.2 核心目标

5.2.1 规范用章流程

建立标准化的用章申请、审批、盖章、归档流程，明确各环节的操作规范与责任主体，避免用章流程的随意性，确保每一次用章行为都符合组织管理规范。

5.2.2 提升管理效率

通过自动化流转、智能提醒、多端操作等功能，缩短用章申请的审批周期，减少人工沟通与跟进成本，让用章管理从“被动等待”变为“主动推进”，提升整体办公效率。

5.2.3 防范用章风险

通过全流程追溯、权限管控、合规校验等机制，防范越权用章、无记录用章、印章滥用等行为，降低因用章不当引发的法律纠纷与经济损失。

5.2.4 实现数据驱动管理

通过采集用章全流程数据，生成多维度统计报表，为组织优化用章管理规范、调整审批流程、合理配置印章资源提供数据支撑，实现管理决策的科学化。

5.3 产品架构

5.3.1 整体架构

系统采用 B/S（Browser/Server）架构，即浏览器/服务器架构，用户无需安装客户端软件，通过主流浏览器（Chrome、Firefox、Edge、Safari 等）即可访问系统，降低部署与维护成本。系统整体架构分为三层：

- 表现层：即用户交互层，包括用户端、审批端、盖章端、管理端四个前端界面，负责接收用户操作请求，展示处理结果，提供直观的操作体验；

- 业务逻辑层：即系统核心层，包含申请管理、审批管理、盖章管理、日志管理、系统设置等核心业务模块，负责处理用户请求，执行业务逻辑，实现流程流转与数据处理；

• 数据访问层：负责与数据库交互，实现数据的存储、查询、修改、删除等操作，支持主流数据库（MySQL、Oracle、SQL Server 等），确保数据存储的稳定性与兼容性。

5.3.2 技术架构

系统采用前后端分离的技术架构，前端基于 Vue.js 框架开发，具备良好的交互体验与响应速度；后端基于 Spring Boot 框架开发，支持高并发、高可用，便于后续功能扩展；数据库采用 MySQL（默认），支持数据的高效存储与查询；服务器采用 Tomcat，支持跨平台部署（Windows、Linux、Unix 等）。

技术架构具备良好的兼容性与扩展性，可根据组织规模与业务需求，灵活调整服务器配置、数据库类型、部署方式，满足不同场景的使用需求。

5.4 产品优势

5.4.1 全流程闭环管理

从用章申请发起，到审批流转、盖章执行、归档存储，形成完整的闭环管理，每一个环节都有记录、可追溯，确保用章管理无遗

漏。

5.4.2 灵活的流程配置

支持可视化流程建模，无需代码开发，管理员可通过拖拽式操作配置审批流程，适配不同用章场景与组织管理规范，灵活应对业务变化。

5.4.3 高强度安全防护

采用多层次安全防护体系，涵盖物理安全、网络安全、数据安全、应用安全，通过加密技术、权限管控、安全审计等机制，确保系统与数据安全。

5.4.4 操作简单易用

界面设计简洁清晰，操作流程标准化，多端适配，无需专业技术知识即可快速上手，降低用户学习成本与组织培训成本。

5.4.5 数据驱动决策

内置多维度统计分析模块，自动采集用章数据，生成可视化报

表，为管理决策提供数据支撑，助力组织持续优化用章管理。

5.4.6 本地化部署与数据自主管控

系统支持本地服务器部署，所有数据存储在组织可控的环境中，符合数据本地化管理要求，确保数据资产的自主管控与安全保密，避免数据泄露风险。

5.5 适用场景

5.5.1 企业日常用章场景

适用于企业内部公文用印、对外合同签署、员工证明文件盖章、财务票据用章、项目方案用章等日常场景，规范用章流程，提升管理效率。例如：销售部门申请合同用章，通过系统发起申请后，流程自动流转至部门主管、法务部、分管领导审批，审批通过后盖章人执行盖章，全程记录可追溯，防范合同用章风险。

5.5.2 事业单位用章场景

适用于事业单位的公文流转用印、审批文件用章、对外合作文件用章、民生服务证明用章等场景，满足合规管理与审计要求。例

如：政务服务中心为群众办理业务时，需为证明文件盖章，通过系统发起申请，经科室负责人、分管领导审批后执行，确保用章行为合规、可追溯。

5.5.3 跨部门协作用章场景

适用于组织内部跨部门协作时的用章需求，如市场部与技术部协作的项目方案用章、财务部与业务部协作的付款文件用章等，通过跨部门审批流程，明确各部门职责，提升协作效率。例如：市场部发起跨部门项目方案用章申请，流程流转至本部门主管、技术部确认、分管领导审批，确保各协作部门达成共识后再执行盖章。

5.5.4 紧急事项用章场景

适用于组织遇到紧急事项（如突发合作、应急处理）时的用章需求，通过紧急申请流程配置，缩短审批周期，快速响应业务需求。例如：企业需紧急签署一份应急采购合同，申请人发起紧急用章申请，系统自动置顶展示，审批人优先处理，确保在短时间内完成审批与盖章，不影响业务推进。

六、系统逻辑结构

6.1 逻辑架构分层

系统逻辑架构遵循“高内聚、低耦合”的设计原则，分为表现层、业务逻辑层、数据访问层、数据存储层四个层级，各层级职责清晰，通过标准化接口交互，确保系统的可扩展性与可维护性。

6.1.1 表现层

表现层是系统与用户的交互接口，负责接收用户操作请求，展示业务数据与处理结果，核心目标是提供友好、便捷的操作体验。表现层按用户角色分为四个前端应用：

- 用户端：面向普通用户，核心功能包括发起用章申请、上传申请材料、查询申请状态、查看审批记录、接收系统通知等；

- 审批端：面向审批人，核心功能包括查看待办审批、处理审批任务（通过/驳回/加签/回退）、查询已办审批、接收审批提醒等；

- 盖章端：面向盖章人，核心功能包括查看待盖章任务、核对申

请信息、上传盖章文件、确认盖章完成、查询盖章记录等；

• 管理端：面向管理员，核心功能包括账号管理、权限配置、流程配置、系统设置、日志管理、统计分析、档案管理等。

表现层采用响应式设计，适配不同屏幕尺寸的设备（PC 端、移动端、平板端），界面元素统一风格，操作流程标准化，确保用户在不同设备上的操作体验一致。

6.1.2 业务逻辑层

业务逻辑层是系统的核心，负责处理用户请求，执行业务规则，实现流程流转与数据处理，是连接表现层与数据访问层的桥梁。业务逻辑层包含八大核心业务模块，各模块独立运行，通过接口协同工作：

• 账号与权限模块：负责用户账号的创建、修改、禁用、密码重置，角色定义、权限分配，登录验证、会话管理等功能；

• 申请管理模块：负责用章申请的接收、数据校验、状态更新、撤回处理、重新提交等功能；

• 审批管理模块：负责审批流程的解析、审批任务的分发、审批操作的处理、流程流转的控制、超时提醒的触发等功能；

• 盖章管理模块：负责盖章任务的接收、状态更新、盖章记录的保存、盖章文件的存储、归档操作的执行等功能；

• 日志管理模块：负责系统所有关键操作的日志记录、日志存储、日志查询、日志导出、日志备份等功能；

• 系统设置模块：负责系统基础参数、安全参数、流程参数的配置与存储，确保系统按预设规则运行；

• 统计分析模块：负责用章数据、审批数据、盖章数据、日志数据的采集、整理、分析，生成统计报表与可视化图表；

• 档案管理模块：负责用章全流程档案的归集、存储、查询、导出、备份等功能，确保档案的完整性与可追溯性。

业务逻辑层采用模块化设计，各模块通过标准化接口交互，例如：申请管理模块接收用户提交的申请后，通过接口将申请数据传递给审批管理模块，审批管理模块解析流程规则后，将审批任务分发至对应审批人，实现跨模块协同。

6.1.3 数据访问层

数据访问层负责与数据存储层交互，提供数据的存储、查询、修改、删除等操作接口，屏蔽数据库类型的差异，确保业务逻辑层无需关注数据存储细节。数据访问层采用 MyBatis 框架开发，通过 XML 配置文件或注解方式定义 SQL 语句，支持主流关系型数据库（MySQL、Oracle、SQL Server 等），便于系统迁移与扩展。

数据访问层的核心功能包括：

- 数据 CRUD 操作：提供对用户表、申请表、审批表、盖章表、日志表、配置表等核心数据表的增删改查操作；

- 数据校验：对数据的完整性、合法性进行校验，确保存入数据库的数据符合预设规则；

- 事务管理：支持数据库事务的控制，确保多步数据操作的原子性（要么全部成功，要么全部失败），例如审批操作与审批日志记录需在同一事务中完成；

- 数据缓存：对高频访问的数据（如角色权限、系统配置参数）

进行缓存处理，提升数据查询效率，减轻数据库压力。

6.1.4 数据存储层

数据存储层负责系统所有数据的持久化存储，包括业务数据、配置数据、日志数据、文件数据等，确保数据的安全性、完整性与可用性。数据存储层分为两部分：

- 数据库存储：采用关系型数据库存储结构化数据，如用户信息、申请信息、审批记录、盖章记录、日志记录、系统配置等，数据库表结构设计遵循第三范式，确保数据冗余最小化，数据一致性最大化；

- 文件存储：采用本地文件系统存储非结构化数据，如申请人上传的原始文件、盖章人上传的盖章文件等，文件存储路径采用加密命名方式，避免路径泄露，同时记录文件元数据（文件 ID、名称、大小、存储路径、哈希值等）至数据库，便于查询与管理。

6.2 核心业务逻辑流程

系统核心业务逻辑流程围绕“用章申请-审批-盖章-归档”的全

生命周期展开，各环节通过数据流转与状态变更实现协同，具体流程如下：

6.2.1 用章申请流程

1. 申请人登录用户端，点击“发起用章申请”，进入申请表单填写页面；

2. 申请人填写基本信息（申请标题、用章用途、所属部门、申请说明等），上传申请材料；

3. 表单填写完成后，申请人点击“提交申请”，系统触发数据校验（必填字段完整性、文件格式与大小合规性）；

4. 校验通过后，数据访问层将申请数据写入申请表，状态设为“待审批”，同时记录申请日志；

5. 系统解析预设的审批流程规则，确定第一个审批节点的审批人；

6. 系统向审批人发送审批提醒（系统内通知+移动端推送），并在审批端待办列表中添加该申请。

6.2.2 审批流转流程

1. 审批人登录审批端，查看待办审批列表，点击申请进入详情页面；

2. 审批人查看申请信息、核验申请材料，填写审批意见，执行审批操作（通过/驳回/加签/回退）；

3. 系统记录审批操作日志，更新申请状态（如“审批中”“已驳回”“待盖章”）；

4. 若操作类型为“通过”：

◦ 系统判断该节点是否为最后一个审批节点；

◦ 若是最后一个节点，申请状态更新为“待盖章”，系统向盖章人发送盖章提醒；

◦ 若不是最后一个节点，系统解析下一审批节点的审批人，推送审批任务，重复步骤 1-3；

5. 若操作类型为“驳回”：

◦ 申请状态更新为“已驳回”，系统向申请人发送驳回通知，告知修改方向；

◦ 申请人修改后可重新提交，流程返回用章申请流程步骤 4；

6. 若操作类型为“加签”：

◦ 系统添加临时审批节点，向加签人推送审批任务；

◦ 加签人审批通过后，流程返回原审批节点，继续流转；

7. 若操作类型为“回退”：

◦ 系统将申请回退至指定前序节点，该节点审批人需重新处理；

◦ 前序节点审批通过后，流程继续向后流转。

6.2.3 盖章与归档流程

1. 盖章人登录盖章端，查看待盖章任务列表，点击申请进入详

情页面；

2. 盖章人核对申请信息与审批记录，确认合规后，线下执行盖章操作；

3. 盖章人上传盖章后的文件，填写盖章记录（盖章时间、地点等），点击“确认完成”；

4. 系统记录盖章操作日志，更新申请状态为“已盖章”，同时触发归档操作：

◦ 数据访问层将申请信息、审批记录、盖章记录、上传文件元数据关联存储，形成完整档案；

◦ 文件存储系统保存盖章后的文件，与原始文件关联；

5. 系统向申请人发送盖章完成通知，告知其可领取文件或查看电子版；

6. 申请人登录用户端，查看申请状态为“已归档”，完成整个用章流程。

6.2.4 异常处理流程

1. 系统运行过程中，若出现数据校验失败、流程配置错误、服务器异常等问题，触发异常捕获机制；

2. 系统记录异常日志（异常类型、发生时间、触发场景、错误信息），并返回友好的错误提示给用户；

3. 管理员通过管理端查看异常日志，定位异常原因：

◦ 若为用户操作错误（如文件格式不符、必填字段未填），通知用户修改后重新操作；

◦ 若为系统配置错误（如审批流程节点缺失），管理员修改配置后，系统自动恢复流程；

◦ 若为服务器或数据库异常，IT 部门排查故障，恢复系统运行；

4. 异常处理完成后，系统更新异常日志的处理状态与处理结果，确保异常处理可追溯。

6.3 数据流转逻辑

系统数据流转遵循“源头唯一、全程共享、状态同步”的原则，数据从申请人发起申请开始，在各环节之间传递与更新，确保数据一致性与完整性。

6.3.1 核心数据实体

系统核心数据实体包括用户、角色、权限、申请、审批、盖章、日志、文件、配置等，各实体的核心字段如下：

- 用户实体：用户 ID、用户名、密码（加密存储）、昵称、所属部门 ID、角色 ID、联系方式、账号状态（启用/禁用）、创建时间、最后登录时间；

- 角色实体：角色 ID、角色名称、角色描述、权限 IDs、创建时间、修改时间；

- 权限实体：权限 ID、权限名称、权限描述、模块名称、操作类型、创建时间；

- 申请实体：申请 ID、申请编号、申请人 ID、申请标题、用章

用途、所属部门 ID、申请说明、联系方式、紧急程度、申请状态、创建时间、提交时间；

• 审批实体：审批 ID、申请 ID、审批人 ID、审批节点、审批意见、操作类型（通过/驳回/加签/回退）、审批时间、流转至下一节点 ID；

• 盖章实体：盖章 ID、申请 ID、盖章人 ID、盖章时间、盖章地点、盖章记录、上传文件 IDs、处理状态、完成时间；

• 日志实体：日志 ID、日志类型（登录/申请/审批/盖章/系统管理）、操作人 ID、操作时间、操作 IP、操作内容、操作结果（成功/失败）、错误信息（失败时）；

• 文件实体：文件 ID、文件名称、文件类型、文件大小、存储路径、哈希值、上传人 ID、上传时间、关联申请 ID、文件状态（正常/已替换/已删除）；

• 配置实体：配置 ID、配置项名称、配置项键名、配置项值、配置描述、创建时间、修改时间。

6.3.2 数据关联关系

各核心数据实体之间通过主键与外键建立关联关系，确保数据流转的连贯性：

• 用户与角色：多对一关系，一个用户关联一个角色，一个角色可关联多个用户；

• 角色与权限：多对多关系，一个角色可关联多个权限，一个权限可关联多个角色（通过角色-权限关联表实现）；

• 申请与申请人：多对一关系，一个申请人可发起多个申请，一个申请关联一个申请人；

• 申请与审批：一对多关系，一个申请可关联多个审批记录（对应不同审批节点），一个审批记录关联一个申请；

• 申请与盖章：一对一关系，一个申请关联一个盖章记录（一个申请仅执行一次盖章操作）；

• 申请与文件：一对多关系，一个申请可关联多个文件（原始文件+盖章文件），一个文件关联一个申请；

• 所有实体与日志：一对多关系，一个实体的操作可产生多个日志记录，一个日志记录关联一个操作实体。

6.3.3 数据状态流转

申请数据的状态流转是数据流转的核心，不同状态对应不同的业务环节，状态变更由系统自动触发或用户操作触发，具体状态流转如下：

• 草稿状态：申请人填写申请信息但未提交，仅保存在本地，未写入数据库；

• 待审批状态：申请人提交申请后，系统生成申请记录，状态设为“待审批”，等待审批人处理；

• 审批中状态：审批人开始处理审批任务，但流程未完成所有审批节点，状态设为“审批中”；

• 已驳回状态：审批人执行“驳回”操作，申请状态设为“已驳回”，等待申请人修改后重新提交；

• 待盖章状态：所有审批节点均通过，申请状态设为“待盖

章”，等待盖章人执行盖章；

• 已盖章状态：盖章人完成盖章操作并确认，申请状态设为“已盖章”；

• 已归档状态：系统自动将已盖章的申请关联所有数据归档，状态设为“已归档”，流程结束。

数据状态的每一次变更都会记录在日志中，包含状态变更前的值、变更后的值、触发人、触发时间，确保状态流转可追溯。

七、适配性与可扩展性

7.1 适配性设计

系统在设计之初充分考虑不同组织的使用场景与环境差异，从硬件、软件、网络、业务四个维度进行适配性设计，确保系统具备广泛的兼容性与适用性。

7.1.1 硬件适配性

系统支持部署在不同规格的硬件设备上，适配从小型服务器到大

型服务器集群的各类硬件配置，满足不同规模组织的使用需求：

• 小型组织：可部署在单台服务器上（推荐配置：CPU≥4 核、内存≥8GB、硬盘≥500GB），支持日均 100 笔以下用章申请的处理；

• 中型组织：可部署在双机热备服务器上（推荐配置：CPU≥8 核、内存≥16GB、硬盘≥1TB），支持日均 100-500 笔用章申请的处理；

• 大型组织：可部署在服务器集群上（推荐配置：CPU≥16 核、内存≥32GB、硬盘≥2TB，支持负载均衡），支持日均 500 笔以上用章申请的处理。

系统支持主流服务器硬件品牌（如戴尔、惠普、华为、联想等），兼容 x86 架构与 ARM 架构服务器，可根据组织硬件资源灵活部署。

7.1.2 软件适配性

系统软件适配性强，兼容主流操作系统、数据库、浏览器，降低部署与维护成本：

• 操作系统：支持 Windows Server（2012 及以上版本）、Linux（CentOS 7 及以上、Ubuntu 18.04 及以上）、Unix 等主流服务器操作系统，无需修改核心代码即可跨平台部署；

• 数据库：支持 MySQL（5.7 及以上）、Oracle（11g 及以上）、SQL Server（2016 及以上）等主流关系型数据库，通过数据访问层的适配接口，实现数据库的无缝切换；

• 浏览器：支持 Chrome（80 及以上）、Firefox（75 及以上）、Edge（80 及以上）、Safari（13 及以上）等主流浏览器，前端界面采用响应式设计，适配不同浏览器的渲染规则，确保操作体验一致；

• 中间件：支持 Tomcat（8.5 及以上）、Jetty（9.4 及以上）等主流 Java Web 服务器，可根据组织习惯选择部署中间件。

7.1.3 网络适配性

系统适配不同的网络环境，确保在局域网、广域网、VPN 等网络场景下均能稳定运行：

• 局域网环境：适用于组织内部办公网络，系统部署在内部服务器，用户通过内部 IP 访问，响应速度快，数据传输安全；

• 广域网环境：支持用户通过互联网访问系统（需部署在公网服务器并配置 HTTPS 与防火墙），适用于异地办公、跨区域协作的组织；

• VPN 环境：支持远程用户通过 VPN 接入内部网络访问系统，确保异地访问的安全性，防止数据泄露；

• 低带宽环境：系统优化数据传输量，减少不必要的资源加载，在带宽较低（≥1Mbps）的网络环境下仍能正常使用核心功能（申请提交、审批处理、文件查看）。

7.1.4 业务适配性

系统支持根据组织业务需求进行灵活配置，适配不同行业、不同规模、不同管理模式的组织：

• 行业适配：通过自定义用章用途、审批流程、合规校验规则，适配企业、事业单位、政府机构、社会组织等不同行业的用章管理需求；

• 规模适配：小型组织可简化流程配置（如“申请人→主管→盖章人”），大型组织可配置复杂流程（如“申请人→部门主管→法务→财务→分管领导→总经理→盖章人”）；

• 管理模式适配：支持集中式管理（所有审批流程、账号权限由总部统一配置）与分布式管理（各分支机构独立配置流程与权限，总部统一监控），适配不同组织的管理模式。

7.2 可扩展性设计

系统采用模块化、标准化的设计理念，具备良好的可扩展性，支持通过功能扩展、接口扩展、部署扩展三种方式，满足组织业务发展与需求变化。

7.2.1 功能扩展

系统核心业务模块采用“插件化”设计，支持在不修改核心代码的前提下，新增功能模块或扩展现有功能：

• 新增功能模块：例如后续可新增“电子印章”模块（支持电子印章生成、电子签章、电子文件加密）、“合同管理”模块（支持

合同模板管理、合同履约跟踪)、“移动端 APP”模块（独立开发移动端 APP，提升移动操作体验）等，新增模块通过标准化接口与现有系统集成，不影响原有功能运行；

• 扩展现有功能：例如在审批管理模块中新增“审批代理”功能(审批人可临时将审批权限委托给他人)、在日志管理模块中新增“日志预警”功能（当出现异常操作时自动向管理员发送预警)，扩展功能通过新增代码模块实现，与原有代码解耦。

系统预留了丰富的功能扩展接口，例如文件预览接口、电子签章接口、第三方系统集成接口等，便于后续快速开发与集成。

7.2.2 接口扩展

系统支持与第三方系统（如 OA 系统、ERP 系统、人事系统、财务系统）进行接口集成，实现数据共享与流程联动，提升组织整体办公效率：

• 数据导入接口：支持从 OA 系统、人事系统导入用户信息、部门架构信息，避免重复录入，确保数据一致性；

• 数据导出接口：支持将用章申请、审批记录、盖章记录导出至

ERP 系统、财务系统，便于后续业务处理（如财务付款、项目归档）；

• 流程联动接口：支持与 OA 系统实现流程联动，例如在 OA 系统中发起用章申请，自动同步至印章审批系统，审批完成后将结果返回 OA 系统，实现“一次申请、全程流转”；

• 单点登录接口：支持与组织现有的统一身份认证系统（如 AD 域、CAS 系统）集成，实现单点登录，用户无需重复输入账号密码，提升操作体验。

接口采用 RESTful API 设计规范，支持 JSON 数据格式，便于第三方系统快速集成。系统提供详细的接口文档，包含接口地址、请求参数、响应格式、错误码说明等，降低集成难度。

7.2.3 部署扩展

系统支持多种部署方式的扩展，满足组织业务增长带来的性能与容量需求：

• 纵向扩展：通过升级服务器硬件配置（增加 CPU 核数、扩大内存、升级硬盘），提升单台服务器的处理能力，适用于用章量中

等且增长平稳的组织；

• 横向扩展：支持服务器集群部署，通过负载均衡设备（如Nginx、F5）将用户请求分发至多台应用服务器，提升系统的并发处理能力与可用性，适用于用章量大、并发用户多的组织；

• 数据库扩展：支持数据库主从复制部署，主数据库负责数据写入，从数据库负责数据查询，减轻主数据库压力；支持数据库分库分表（按时间、部门等维度），适用于数据量庞大的组织；

• 文件存储扩展：当文件存储量较大时，可将文件存储迁移至分布式文件系统（如HDFS、MinIO），提升文件存储的容量与访问速度。

部署扩展过程中，系统核心代码无需修改，仅需调整部署配置与环境参数，确保扩展过程简单、高效。

八、国家标准与合规性说明

印章审批系统V1.0的开发与设计严格遵循国家相关法律法规与行业标准，确保系统的合规性与合法性，满足组织内部管理规范与外部监管要求。

8.1 遵循的国家标准与行业标准

系统开发过程中，严格遵循以下国家标准与行业标准，确保系统功能、技术架构、数据安全等方面符合规范：

8.1.1 信息技术相关标准

• GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》：系统按二级等保标准设计，在物理安全、网络安全、数据安全、应用安全等方面满足等级保护要求；

• GB/T 35273-2020《信息安全技术 个人信息安全规范》：规范用户个人信息（如姓名、联系方式、所属部门）的收集、存储、使用、传输等行为，确保个人信息安全；

• GB/T 19001-2016《质量管理体系要求》：遵循质量管理体系标准，确保系统开发过程的规范性、产品质量的可靠性；

• GB/T 28181-2016《公共安全视频监控联网系统信息传输、交换、控制技术要求》：机房视频监控系统符合该标准，确保物理安全监控的合规性。

8.1.2 电子政务与办公相关标准

• GB/T 9704-2012《党政机关公文格式》：系统内公文用章申请的表单设计、文件上传格式要求符合该标准，确保公文处理的规范性；

• GB/T 33190-2016《电子文件管理基本术语》：系统电子档案的管理遵循该标准，明确电子文件的归档、存储、检索等术语与要求；

• GB/T 33900-2017《电子文件归档与管理规范》：电子档案的归档范围、归档时间、存储格式、保管期限等符合该标准，确保电子档案的可用性与可追溯性。

8.1.3 个人信息保护法合规实现

《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）明确规定了个人信息处理的合法性、正当性、必要性原则，系统在设计与开发过程中，严格遵循该法对个人信息收集、存储、使用、加工、传输、提供、公开等环节的要求，构建全流程个人信息保护机制。

8.1.3.1 个人信息范围界定与最小化收集

系统处理的个人信息主要包括用户账号信息（用户名、昵称、所属部门、角色）、身份验证信息（密码哈希值）、联系方式（手机号）、操作轨迹信息（登录 IP、设备信息、操作日志）等，均为支撑系统核心功能运行所必需的信息，无冗余收集。

在信息收集环节，严格遵循“最小必要”原则：仅收集与用章审批业务直接相关的个人信息，不收集与业务无关的敏感信息（如身份证号、银行卡号、生物识别信息等）；所有个人信息均通过系统内部表单主动填报，不存在隐蔽收集或强制授权收集的情况；用户联系方式等可选信息，允许用户根据实际需求选择是否提供，不将其作为使用系统核心功能的前置条件。

8.1.3.2 个人信息处理的合法性保障

系统处理个人信息的合法性基础主要包括“经个人同意”与“为履行法定职责或合同义务所必需”：用户首次登录系统并接受《用户使用协议》时，即视为同意系统按照协议约定处理其个人信息；用章申请、审批流转等业务环节中，个人信息的处理是完成组织内部业务协作的必要前提，符合“为履行合同义务所必

需”的合法性要求。

系统在《用户使用协议》中明确告知用户个人信息的处理目的、处理方式、存储期限、安全保护措施等核心内容，保障用户的知情权；用户有权通过联系管理员的方式，查询、更正自身的个人信息（如昵称、联系方式），若用户离职或不再使用系统，可申请删除个人账号及相关信息，管理员核实后将执行账号注销与信息匿名化处理，保障用户的个人信息权利。

8.1.3.3 个人信息存储与安全保护

系统所有个人信息均存储于部署单位本地受控环境，采用“加密存储+权限隔离”的双重保护机制：用户密码等敏感信息采用SHA-256不可逆哈希算法加密后存储，不存储明文信息；手机号等标识性个人信息采用字段级加密处理，加密密钥由部署单位专人保管，仅授权账号可通过解密接口访问。

个人信息的存储期限严格遵循“必要最短”原则：账号处于正常状态时，个人信息将持续存储以保障系统使用；账号注销或用户离职后，个人信息将在完成业务追溯所需的最短周期内（默认不超过6个月）完成匿名化处理，删除可识别个人身份的标识信息，仅保留用于业务统计分析的脱敏数据。

系统通过严格的权限控制，限制个人信息的访问范围：普通用户仅能查看自身的个人信息；审批端与盖章端仅能查看与审批、盖章业务相关的必要个人信息（如申请人姓名、联系方式）；管理端管理员需具备专门的个人信息访问权限，且所有访问操作均记录在审计日志中，确保个人信息不被非法访问或滥用。

8.1.3.4 个人信息处理的合规审计

系统建立个人信息处理合规审计机制，定期对个人信息收集、存储、使用、删除等全流程操作进行审计。审计内容包括：个人信息收集是否符合最小必要原则、存储是否采用加密措施、访问权限是否合理、删除是否及时彻底等。审计结果将形成合规审计报告，由部署单位安全管理部门留存，作为应对监管检查的重要依据。

若发生个人信息泄露、丢失等安全事件，系统将通过日志快速定位事件原因与影响范围，并按照《个人信息保护法》要求，及时向部署单位负责人报告，必要时通知受影响用户，并采取补救措施，降低事件造成的损失。

8.1.4 电子签名法合规实现

《中华人民共和国电子签名法》为电子签名、数据电文的法律效力提供了明确依据，系统在设计中充分考虑电子证据的合法性要求，确保用章审批过程中形成的电子记录、电子文件具备与纸质文件同等的法律效力。

8.1.4.1 电子记录的真实性与完整性保障

系统对用章申请、审批流转、盖章归档等全流程产生的电子记录进行完整性保护：所有电子记录（包括申请信息、审批意见、操作日志等）均采用时间戳+哈希值双重校验机制，时间戳由系统本地时钟生成（同步部署单位授时服务器，确保时间准确性），哈希值采用 SHA-256 算法计算，每一条电子记录的哈希值与记录内容绑定存储，任何对记录内容的篡改都将导致哈希值不一致，系统可通过校验哈希值快速识别记录是否被篡改。

电子记录的生成过程完全自动化，不存在人工干预修改的可能：申请信息由用户提交后自动写入数据库，审批意见由审批人在线填写后即时保存，操作日志由系统后台自动记录，所有电子记录均包含操作人、操作时间、操作设备等关键标识信息，确保记录的可追溯性。

8.1.4.2 电子文件的合规性处理

对于用户上传的申请材料、盖章端上传的盖章文件等电子文件，系统在存储过程中保留文件的原始格式与元数据信息（如文件创建时间、修改时间、文件哈希值等），不进行任何破坏性编辑或格式转换，确保电子文件的原始性。

系统支持对电子文件进行完整性校验，用户、审批人、管理员均可通过系统功能查看电子文件的哈希值，验证文件是否在传输或存储过程中被篡改。若需要将电子文件作为法律证据使用，系统可导出包含文件元数据、哈希值、相关电子记录的完整证据包，配合部署单位的公章使用记录，形成完整的证据链，满足《电子签名法》对电子证据的要求。

8.1.4.3 电子签名相关功能预留

虽然系统V1.0版本暂未启用电子签名功能，但在架构设计中预留了电子签名接口，支持未来集成符合《电子签名法》要求的第三方电子签名服务（如具备《电子认证服务许可证》的CA机构提供的服务）。启用电子签名功能后，审批人可通过电子签名确认审批意见，盖章端可通过电子签章完成线上盖章，电子签名、电子签章的生成、验证过程将严格遵循《电子签名法》规定，确

保其法律效力。

8.2 信息安全等级保护要求

根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239）的相关规定，结合系统的业务性质、数据敏感性及影响范围，建议部署单位将本系统定级为二级等级保护对象（以下简称“等保二级”）。等保二级适用于面向内部或特定外部群体提供服务、对公民、法人和其他组织的合法权益有一定影响，但不影响国家安全、社会秩序和公共利益的一般业务系统，与本系统的应用场景高度匹配。

系统在设计阶段已充分考虑等保二级的技术要求，预留了对应的实施节点，部署单位在实施过程中需结合等保二级要求完成定级备案、差距整改、等级测评等工作，确保系统满足等保二级的各项控制要求。以下为系统针对等保二级核心技术要求的设计实现：

8.2.1 网络边界安全

系统支持部署在部署单位的内部局域网或专用网络中，通过网络边界设备（如防火墙、入侵防御系统）划分安全区域，将系统服

务器所在区域与互联网、其他非信任区域隔离，仅开放必要的网络端口（如 HTTP/HTTPS 端口），关闭不必要的服务与端口，防范外部网络攻击。

对于远程运维、跨区域访问等场景，系统支持通过 VPN（虚拟专用网络）实现安全接入，VPN 采用强加密协议（如 IPsec、SSL VPN）对传输数据进行加密，同时配置访问白名单，仅允许授权的 IP 地址、设备接入，确保远程访问的安全性。

系统支持与部署单位的网络安全设备（如入侵检测系统、日志审计系统）对接，将系统的网络访问日志、操作日志实时推送至网络安全设备，便于安全管理人员实时监控网络访问行为，及时发现异常流量与攻击行为。

8.2.2 主机安全

系统推荐部署在 Linux 服务器环境中，服务器操作系统需进行安全加固：关闭不必要的系统服务（如 FTP、Telnet）、禁用默认账号、修改默认端口、配置文件权限最小化、开启系统日志审计功能等，降低主机被攻击的风险。

服务器配备防病毒软件，定期更新病毒库，对服务器文件进行实

时查杀，防范恶意代码、病毒感染；同时，建立服务器补丁管理机制，定期检查操作系统、中间件（如 Nginx、Apache）的安全补丁，及时安装必要的补丁，修复已知安全漏洞。

系统采用专用账号运行应用服务，该账号仅具备运行应用所需的最小权限，不具备服务器管理员权限，避免应用服务被劫持后导致服务器被非法控制；服务器的文件系统采用权限隔离设计，系统程序文件、配置文件、数据文件分别存储在不同目录，设置不同的访问权限，防止数据文件被非法修改或删除。

8.2.3 身份鉴别与权限管理

系统的身份鉴别与权限管理功能完全符合等保二级要求：采用用户名+密码的身份鉴别方式，密码满足复杂度要求（长度不少于 12 位，包含四种字符类型），支持定期更换；登录失败达到阈值后自动锁定账号，记录登录失败日志；系统会话标识采用随机字符串生成，有效期可配置，会话超时后自动退出登录，防止账号被冒用。

权限管理采用 RBAC 模型，基于岗位与职责分配权限，实现权限的精细化管控；所有权限变更操作均记录日志，包含变更人、变更时间、变更内容等信息；定期对用户权限进行审计，清理冗余

权限、过期权限，确保权限分配的合理性。

对于管理端的重要操作（如账号创建、权限修改、系统配置变更），系统支持配置双人确认机制，需两名具备相应权限的管理员共同操作才能完成，防止单人操作导致的误操作或恶意操作风险。

8.2.4 日志审计

系统建立了全面的日志审计机制，日志类型包括登录日志、操作日志、系统日志、安全日志等，覆盖系统运行的全流程。日志记录包含操作人、操作时间、操作类型、操作对象、操作结果、IP地址、设备信息等详细字段，确保所有操作行为均可追溯。

日志采用追加写入策略，不允许删除或修改已生成的日志记录；日志存储在本地受控目录，支持按时间分区存储，存储期限可配置（默认不少于1年），满足等保二级对日志留存时间的要求；日志支持导出功能，导出格式为CSV或Excel，便于安全管理人员进行日志分析与审计。

部署单位可将系统日志接入第三方日志审计平台，实现日志的集中管理、分析与告警，通过日志分析工具挖掘异常操作行为、潜

在安全风险，为安全事件处置提供依据。

8.2.5 数据备份与恢复

系统建立了完善的数据备份与恢复机制，确保数据的可用性与完整性。数据备份包括数据库备份与文件备份：数据库采用定时备份策略，支持全量备份与增量备份结合（如每天增量备份，每周全量备份），备份数据存储在独立的备份服务器或存储设备中，与生产数据隔离；文件备份采用同步备份方式，用户上传的文件实时同步至备份存储设备，防止文件丢失。

备份数据进行加密存储，备份介质由专人保管，定期进行备份数据的可用性验证，确保备份数据能够正常恢复；建立数据恢复流程，明确数据恢复的触发条件、操作步骤、责任人等，定期组织数据恢复演练，确保在数据丢失、损坏时能够快速恢复数据，将业务中断时间降至最低。

8.2.6 等保二级实施流程建议

部署单位应按照以下流程完成等保二级实施工作：

1. 定级备案：向当地公安机关网络安全保卫部门提交定级备案

材料，包括定级报告、系统说明、安全管理制度等，完成备案手续；

2. 差距整改：对照等保二级要求，对系统的技术架构、安全配置、管理制度等进行全面梳理，找出差距并进行整改，如补充安全设备、优化权限配置、完善管理制度等；

3. 等级测评：委托具备资质的等级测评机构对系统进行等级测评，出具等级测评报告；

4. 持续改进：根据等级测评报告的整改建议，进一步完善系统安全防护措施，建立安全长效机制，定期进行安全评估与整改。

8.3 国家标准与行业规范参考

系统在设计与开发过程中，严格遵循信息安全领域的相关国家标准与行业规范，确保系统的技术实现、安全防护、数据处理等方面符合行业通用要求。以下为系统主要参考的国家标准与行业规范：

8.3.1 网络安全等级保护相关标准

• 《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)：该标准规定了网络安全等级保护的安全技术要求和安全管理要求，是系统安全设计的核心依据，系统的网络边界安全、主机安全、身份鉴别、权限管理、日志审计等功能均按照该标准的二级要求进行设计；

• 《信息安全技术 网络安全等级保护测评要求》(GB/T 25070-2019)：该标准规定了网络安全等级保护测评的内容和方法，为系统的安全测试与等级测评提供了依据，系统的测试方案、安全评估流程均参考该标准制定；

• 《信息安全技术 信息安全等级保护定级指南》(GB/T 28448-2019)：该标准规定了信息系统等级保护的定级原则、定级流程和定级方法，系统的等保定级工作主要依据该标准开展；

• 《信息安全技术 网络安全等级保护实施指南》(GB/T 28449-2019)：该标准提供了网络安全等级保护的实施流程、技术方案和管理措施，为系统的安全实施、部署配置、运维管理提供了参考。

8.3.2 个人信息保护相关标准

• 《信息安全技术 个人信息安全规范》(GB/T 35273-2022)：该标准规定了个人信息处理的安全要求，包括个人信息的收集、存储、使用、传输、删除等环节，系统的个人信息保护功能（如最小化收集、加密存储、权限控制）均按照该标准进行设计；

• 《信息安全技术 个人信息安全影响评估指南》(GB/T 39335-2020)：该标准提供了个人信息安全影响评估的流程和方法，系统部署前，部署单位可参考该标准开展个人信息安全影响评估，识别个人信息处理过程中的风险，制定应对措施。

8.3.3 电子证据相关标准

• 《信息安全技术 电子数据取证指南》(GB/T 29361-2023)：该标准规定了电子数据取证的原则、流程和方法，系统的日志记录、电子文件存储、哈希值校验等功能设计参考了该标准，确保电子数据具备取证价值；

• 《信息安全技术 电子签名格式规范》(GB/T 25064-2022)：该标准规定了电子签名的格式要求和验证方法，系统预留的电子签名接口按照该标准进行设计，为未来启用电子签名功能提供合规保障。

8.3.4 行业规范参考

系统参考了公安行业关于印章管理信息系统的相关行业规范，重点关注印章使用的备案管理、追溯管理、安全管理等要求，确保系统的用章审批流程、印章使用记录、安全防护措施符合行业管理要求。

若部署单位需要将系统与公安机关印章管理监管平台对接，可根据监管平台的接口规范、数据格式要求，对系统的数据输出格式、接口参数进行适配，确保数据能够正常上报，满足监管要求。

8.4 证据保全与电子数据可信性说明

系统在设计中充分考虑电子数据的证据价值，通过技术手段确保用章审批过程中形成的电子记录、电子文件具备真实性、完整性、可追溯性，能够在法律程序中作为有效电子证据使用。

8.4.1 电子证据链的构建

系统构建了完整的电子证据链，将用章申请、审批、盖章、归档等各环节的相关数据进行关联，形成闭环证据体系。电子证据链

的核心组成部分包括：

1. 申请环节：用章申请表单信息（申请标题、用章用途、所属部门等）、申请材料电子文件及元数据、申请提交日志（提交人、提交时间、提交设备等）；

2. 审批环节：审批记录（审批人、审批时间、审批意见、审批结果）、审批流转日志、审批编号（唯一标识）；

3. 盖章环节：盖章文件电子文件及元数据、盖章上传日志（上传人、上传时间、设备信息）；

4. 系统运行环节：登录日志、操作日志、系统配置日志、安全日志。

以上所有数据通过审批编号进行唯一关联，形成“申请-审批-盖章-归档”的完整证据链，任何环节的操作都将被记录并关联至该证据链，确保每一次用章行为都可精准追溯源头与全过程。

8.4.2 电子数据的可信性保障

为确保电子数据的可信性，系统采用“技术加密+流程管控+日志

固化”三重保障机制，从数据生成、存储、传输到使用全流程防范篡改、伪造风险，确保电子数据满足法律对证据的核心要求：

8.4.2.1 真实性保障技术

• 身份绑定机制：所有电子数据的生成均与授权用户账号强绑定，申请信息由申请人账号提交后自动写入数据库，审批意见由审批人账号在线签署后即时留存，盖章文件由盖章端账号上传后关联至对应审批记录，操作人身份信息（用户名、所属部门、角色）将永久嵌入数据元信息，确保数据来源可精准追溯，杜绝匿名操作或身份冒用导致的数据失真。

• 时间戳精准固化：系统内置时间同步机制，所有电子数据生成时均自动关联精准时间戳，时间戳同步部署单位内部授时服务器(支持对接国家授时中心服务器校准)，精确到毫秒级，确保申请提交时间、审批处理时间、文件上传时间等关键时间节点的真实性，避免人为修改系统时间导致的时间造假。时间戳信息与数据内容绑定存储，作为电子数据生成时序的核心证明依据。

• 操作轨迹全程留痕：用户在系统内的每一项操作（如修改申请信息、补充审批意见、替换上传文件）都将生成操作轨迹记录，包含操作前数据状态、操作后数据状态、操作时间、操作设备

IP 等信息，形成“原始数据-操作变更-最终状态”的完整轨迹链，即使数据发生合法变更，也可通过轨迹记录还原变更全过程，保障数据变更的可追溯性。

8.4.2.2 完整性保障技术

• 哈希值双重校验：系统对所有核心电子数据（包括申请表单信息、审批记录、电子文件、操作日志）均采用 SHA-256 加密算法计算唯一哈希值，哈希值与数据内容一一对应，存储于独立的校验数据库中，与业务数据物理隔离。用户、审批人或审计人员可通过系统内置的校验工具，随时对电子数据进行哈希值校验，若数据内容被篡改（包括恶意修改、传输错误、存储损坏等），校验结果将显示哈希值不匹配，即时发现数据完整性问题。

• 数据传输加密：电子数据在客户端与服务器之间传输时，采用 HTTPS 协议（TLS 1.3 版本）进行端到端加密，所有数据传输包均经过加密处理，防止数据在传输过程中被拦截、篡改或伪造，确保数据从用户提交到服务器存储的传输过程中保持完整。

• 文件完整性校验：对于用户上传的申请材料、盖章端上传的盖章文件，系统除计算文件整体哈希值外，还对文件的关键元数据（如文件大小、创建时间、修改时间）进行校验存储，上传完成

后自动比对元数据与文件内容的一致性，若文件在上传过程中发生损坏或被替换，系统将自动拒绝存储并提示用户重新上传，保障存储文件的完整性。

8.4.2.3 不可篡改性保障技术

• 日志追加写入与只读保护：系统所有操作日志（登录日志、业务操作日志、安全日志）均采用“追加写入”模式，日志文件设置为只读权限，仅允许系统后台进程写入新日志，不允许任何用户（包括系统管理员）修改、删除已生成的日志记录。日志文件采用分区存储策略，按天或按月生成独立日志文件，生成后自动加密归档，进一步防范日志被篡改的风险。

• 核心业务数据写保护：审批记录、审批编号、时间戳等核心业务数据写入数据库后，系统自动为其设置写保护标记，仅支持查询操作，不支持直接修改操作。若因业务特殊需求（如司法机关要求更正错误信息）需修改核心数据，必须通过管理端的“数据更正审批流程”，由两名以上管理员审批通过后，系统生成更正日志（记录更正原因、更正人、更正时间、原始数据、更正后数据），并保留原始数据的完整备份，确保核心数据的修改过程可追溯、原始数据不丢失。

• 存储介质安全隔离：系统业务数据、校验数据、日志数据分别存储在独立的存储介质中，数据库服务器与文件存储服务器物理分离，且均部署在部署单位的本地受控环境中，配置严格的访问权限控制，仅授权的应用服务账号可访问，防止存储介质被非法访问导致的数据篡改。

8.4.3 电子证据的司法适配性

系统生成的电子数据在设计时充分考虑司法实践中对电子证据的采信要求，可通过以下方式提升电子证据的司法认可度：

• 证据包标准化导出：系统支持将某一审批流程的完整电子证据链导出为标准化证据包，证据包包含 PDF 格式的证据清单（列明证据组成、生成时间、关联关系）、各环节电子数据的原始文件（申请表单、审批记录、盖章文件等）、对应的哈希值校验报告、操作日志截图等，所有文件按“申请-审批-盖章-归档”流程分类整理，便于司法机关查阅核验。

• 第三方证据保全对接：系统预留第三方证据保全接口，支持与具备司法认证资质的电子证据保全平台（如公证处电子证据保全系统、区块链存证平台）对接。部署单位可根据需求，将关键审批流程的电子数据实时同步至第三方保全平台，由第三方平台提

供时间戳认证、区块链存证等服务，形成“系统生成+第三方保全”的双重证据效力，进一步提升电子证据的司法采信度。

• 审计报告出具支持：系统可根据审计需求，生成包含电子数据生成流程、安全防护措施、哈希值校验结果、日志记录摘要等内容的审计报告，审计报告由系统自动生成并加盖管理端电子签章(若启用)，明确报告生成时间、生成主体，可作为电子数据可信性的辅助证明材料，用于内部审计或外部监管检查。

8.4.4 电子数据的保全与销毁规范

8.4.4.1 电子数据保全策略

• 定期备份与归档：系统采用“实时增量备份+定期全量备份”的备份策略，数据库每天进行增量备份，每周进行全量备份，备份数据存储在加密的备份服务器中，备份周期可由管理端配置(默认不少于 1 年)。超过存储期限的电子数据，系统自动进行归档处理，归档数据采用压缩加密存储，存储介质由部署单位专人保管，建立归档台账，记录归档时间、存储位置、责任人等信息。

• 异地容灾备份（可选）：对于数据安全性要求较高的部署单

位，系统支持异地容灾备份配置，将备份数据同步存储至异地备份中心，备份中心与主存储环境物理隔离，采用相同的安全防护措施，确保在主存储环境发生自然灾害、设备故障等意外情况时，可通过异地备份数据快速恢复，保障电子数据的长期可用性。

8.4.4.1 电子数据销毁规范

• 销毁触发条件：电子数据的销毁仅在以下情况下触发：① 超过法定存储期限（根据部署单位所属行业的监管要求确定，如一般企业不低于 3 年，政府机关不低于 5 年）；② 部署单位因业务调整不再需要该部分数据，且已完成司法取证、审计等相关工作；③ 用户注销账号后，相关个人信息已完成匿名化处理，剩余业务数据无留存必要。

• 销毁流程与方式：电子数据销毁需通过管理端的“数据销毁审批流程”，由业务部门、安全管理部门、技术部门共同审批通过后执行。销毁方式采用“物理删除+数据覆写”双重方式：对于数据库中的数据，执行物理删除操作后，对存储区域进行多次随机数据覆写，防止通过数据恢复技术还原；对于文件存储中的数据，删除文件后对存储目录进行磁盘擦除操作，确保数据彻底销毁。销毁过程生成销毁日志，记录销毁数据范围、销毁时间、审

批人、执行人等信息，归档留存备查。

九、实施与交付

系统实施与交付是确保系统从技术开发完成到实际落地应用的关键环节，本章节详细描述系统实施的全流程、标准化交付物清单以及专项培训与上线支持方案，确保部署单位能够快速、平稳地启用系统，充分发挥系统的管理价值。

9.1 实施流程

系统实施遵循“需求驱动、分步落地、全程可控”的原则，划分为需求确认、环境准备、系统安装、数据迁移、测试验证、培训赋能、验收上线七个核心阶段，每个阶段明确目标、责任主体与交付成果，确保实施过程有序推进。

9.1.1 需求确认阶段

需求确认是实施工作的起点，旨在明确部署单位的个性化需求，确保系统配置与业务实际高度匹配。实施团队与部署单位指定的项目负责人、业务骨干、技术负责人共同成立需求确认小组，通过现场调研、专题会议、需求问卷等方式，完成以下核心需求的

收集与确认：

• 组织架构与账号策略：明确部署单位的部门层级架构（如总部-分公司-部门-班组）、各部门职责分工、用户数量及岗位设置；确定账号命名规则、初始密码分配方式、密码有效期、登录失败锁定阈值等账号管理策略；明确不同岗位的角色划分及权限需求（如是否需要增设“法务审批角色”“部门管理员角色”等自定义角色）。

• 审批流程定义：根据部署单位的用章管理规定，明确用章申请的审批流程配置，包括：① 审批节点设置（如部门负责人审批→法务审批→分管领导审批→盖章端确认）；② 审批权限分配（明确各节点审批人的所属部门、角色范围）；③ 审批规则配置（如紧急申请的审批时效要求、大额合同用章的多级审批要求、特殊用章用途的额外审批节点）；④ 驳回规则定义（驳回后是否返回申请人修改、是否需要重新经过所有审批节点）。

• 表单与编号规则：确认用章申请表单的字段配置（如是否需要增加“项目编号”“合同金额”等自定义字段、哪些字段为必填项）；确定审批编号的生成规则（前缀字符、年份格式、部门代号编码规则、流水号位数等），如“ORG-2024-DEP01-00001”（ORG 为固定前缀，2024 为年份，DEP01 为部门代号，00001 为流

水号）。

• 数据管理与安全需求：明确电子数据的存储期限（如审批记录、操作日志的留存时间）、备份周期与备份方式；确定文件上传的大小限制、支持格式；明确是否需要对接第三方系统（如OA系统、档案管理系统）、是否需要启用异地容灾备份等安全需求。

需求确认完成后，实施团队编制《需求确认说明书》，明确需求范围、配置方案、实施优先级，经双方签字确认后作为后续系统配置、测试验收的依据，避免实施过程中因需求变更导致的工期延误。

9.1.2 环境准备阶段

环境准备阶段的目标是搭建符合系统运行要求的硬件、软件与网络环境，确保系统安装部署后能够稳定运行。实施团队提供《环境准备指南》，明确环境配置要求，由部署单位的IT部门负责环境搭建，实施团队提供技术指导：

• 硬件环境准备：根据系统部署模式（单机部署/主备部署/集群部署），准备相应的服务器设备：① 应用服务器：推荐配置4核

CPU、8GB 内存、1TB SSD 存储（单机部署），集群部署时需根据并发用户数扩容（如 1000 并发用户需配置 8 核 CPU、16GB 内存）；② 数据库服务器：推荐配置 8 核 CPU、16GB 内存、2TB 存储，采用企业级硬盘（如 SAS 硬盘）确保数据存储稳定性；③ 备份服务器：配置与主服务器相当的存储容量，用于数据备份与归档；④ 网络设备：确保服务器所在网络带宽不低于 100Mbps，延迟低于 50ms，配置防火墙、路由器等网络设备，开放系统所需端口（如 80 端口、443 端口、3306 端口）。

• 软件环境准备：① 操作系统：应用服务器与数据库服务器推荐安装 Linux 发行版（如 CentOS 7.9、Ubuntu 20.04），确保操作系统已完成安全加固（关闭不必要服务、禁用默认账号等）；② 中间件：Web 服务器推荐安装 Nginx 1.20 及以上版本或 Apache 2.4 及以上版本，配置 HTTPS 协议；③ 数据库：安装 MySQL 5.7 或 MariaDB 10.5 及以上版本，启用数据库日志功能（二进制日志、慢查询日志），配置数据库连接池参数；④ 依赖组件：安装 PHP 8.0 及以上版本，配置 PHP 运行环境（如内存限制、上传文件大小限制），安装 GD 库、OpenSSL 等必要扩展组件。

• 安全环境准备：部署单位 IT 部门配置网络防火墙规则，仅允许授权 IP 地址访问服务器；启用服务器防病毒软件，更新病毒

库；配置存储介质加密（如磁盘分区加密）；建立服务器账号管理制度，为系统运行创建专用服务账号，分配最小权限；准备SSL证书（从权威CA机构申请），用于HTTPS协议配置。

环境搭建完成后，实施团队与部署单位IT部门共同进行环境验收，填写《环境验收报告》，确认硬件配置、软件版本、网络连通性、安全配置等符合系统运行要求后，进入下一阶段。

9.1.3 系统安装阶段

系统安装阶段由实施团队负责，基于已确认的《需求确认说明书》和验收通过的运行环境，完成系统部署与初始化配置：

• 安装部署流程：① 服务器环境检查：实施团队通过远程登录或现场操作，检查服务器的软件版本、依赖组件、端口占用情况，确保安装环境符合要求；② 数据库初始化：执行数据库脚本，创建系统所需的数据库、数据表、索引、存储过程等，配置数据库用户权限（仅授予系统服务账号必要的查询、插入、更新权限）；③ 应用程序部署：将系统安装包上传至应用服务器，解压至指定目录，配置Web服务器（如Nginx的虚拟主机配置、PHP运行参数），建立应用程序与数据库的连接；④ 系统参数配置：登录管理端，根据《需求确认说明书》配置系统核心参数，

包括组织架构信息、角色权限模板、审批流程节点、表单字段配置、审批编号规则、文件存储路径、日志留存期限等；⑤ 初始账号创建：创建系统超级管理员账号、各部门管理员账号、测试账号，分配初始密码，记录账号信息并移交部署单位。

• 安全配置强化：① 配置 HTTPS 协议：安装 SSL 证书，修改 Web 服务器配置，强制所有访问通过 HTTPS 协议，禁用 HTTP 协议；② 优化密码策略：在管理端配置密码复杂度要求、有效期、登录失败锁定阈值等；③ 文件权限设置：修改系统程序文件、配置文件、文件存储目录的访问权限，仅允许服务账号读写，禁止其他账号访问；④ 数据库安全配置：修改数据库默认端口，禁用远程 root 登录，配置数据库连接超时时间，启用数据库加密功能（如数据传输加密、敏感字段存储加密）。

系统安装完成后，实施团队进行安装自检，验证系统是否能正常启动、数据库连接是否正常、核心功能是否可正常使用，填写《系统安装报告》，记录安装过程、配置参数、自检结果。

9.1.4 数据迁移阶段

若部署单位存在传统纸质用章记录或旧系统电子数据，实施团队提供数据迁移服务，将历史数据导入新系统，确保数据的连续性

与完整性。数据迁移遵循“数据清洗-格式转换-导入验证-备份留存”的流程：

• 数据梳理与清洗：部署单位负责整理历史数据，包括纸质记录扫描件、旧系统数据导出文件（如 Excel、CSV 格式），明确数据字段与新系统字段的对应关系（如旧系统“申请部门”对应新系统“所属部门”）。实施团队协助进行数据清洗，剔除重复数据、无效数据（如缺失关键字段的数据），修正数据格式错误（如日期格式统一、部门名称标准化），确保迁移数据符合新系统的数据规范。

• 数据格式转换：实施团队根据新系统的数据结构，编写数据迁移脚本，将清洗后的历史数据转换为新系统可识别的格式。对于纸质记录扫描件，转换为 PDF 或图片格式，按“年份-部门-申请编号”的规则命名，确保文件可与电子记录关联；对于旧系统电子数据，通过脚本批量转换字段格式、映射部门与角色信息，确保数据迁移后可正常查询与使用。

• 数据导入与验证：实施团队通过数据库导入工具或自定义脚本，将转换后的历史数据批量导入新系统。导入完成后，采用“抽样验证+全量校验”的方式进行数据验证：① 抽样验证：随机抽取不同部门、不同时间段的历史数据，对比新系统中的数据

与原始数据的一致性，包括字段内容、文件关联、审批记录等；② 全量校验：通过脚本校验导入数据的总数与原始数据总数是否一致，校验核心字段（如审批编号、申请人、申请时间）的完整性，确保无数据丢失或重复导入。

• 历史数据备份：数据迁移完成后，实施团队将原始历史数据（纸质记录扫描件、旧系统导出文件）进行压缩加密备份，存储在部署单位指定的存储介质中，建立备份台账，确保历史数据可追溯。

数据迁移完成后，实施团队编制《数据迁移报告》，记录数据迁移流程、数据量、清洗情况、验证结果、备份情况，经双方确认后归档。

9.1.5 测试验证阶段

测试验证阶段旨在全面检测系统的功能完整性、性能稳定性、安全可靠性，确保系统满足部署单位的业务需求与安全要求，为系统上线提供坚实保障。测试工作由实施团队、部署单位业务骨干、IT 部门共同组成测试小组，遵循“全覆盖、无死角、可复现”的测试原则，分为功能测试、性能测试、安全测试、兼容性测试四个维度，测试过程全程记录，缺陷闭环管理。

9.1.5.1 功能测试

功能测试是测试验证的核心环节，基于《需求确认说明书》《系统功能清单》及部署单位个性化需求，设计详细的测试用例，覆盖系统所有核心功能模块及边缘场景，确保功能实现与需求一致。

• 测试范围与用例设计：

◦ 账号与权限管理模块：覆盖账号创建、信息编辑、状态启用/禁用、密码修改、角色分配、权限校验、登录失败锁定、历史登录记录查询等功能，设计用例包括“创建含特殊字符的用户名是否成功”“修改用户所属部门后权限是否同步更新”“禁用账号后能否登录系统”“越权访问管理端功能是否被拦截”等，覆盖正常操作与异常场景。

◦ 登录功能模块：测试用户名/密码正确登录、错误密码登录、锁定账号登录、会话超时自动退出、HTTPS 协议访问是否生效等场景，验证登录日志记录的完整性与准确性。

◦ 用章申请提交模块：测试表单必填字段校验、格式校验（如手

机号、日期格式）、文件上传（不同格式、大小、数量的文件）、申请提交、撤回、修改等功能，验证申请信息、文件元数据、提交日志的一致性。

◦ 审批管理模块：测试待办审批推送、审批通过/驳回操作、驳回意见必填校验、审批记录生成、审批链追溯、审批编号自动生成（含并发场景）、审批记录检索等功能，验证审批流程与配置规则一致。

◦ 盖章文件上传模块：测试盖章文件与审批记录绑定、文件上传校验、状态更新为“已归档”、上传日志记录等功能，验证盖章文件元数据的完整性。

◦ 日志与审计模块：测试登录日志、操作日志、系统日志的记录完整性，日志查询（多条件筛选）、导出（不同格式）功能，验证日志不可篡改特性。

◦ 管理端配置模块：测试组织架构维护、角色权限配置、审批流程调整、编号规则修改、系统参数设置等功能，验证配置变更后即时生效且记录变更日志。

• 测试执行与缺陷管理：

测试小组按测试用例逐一对功能进行验证，记录测试结果（通过/失败）、实际执行效果、异常现象截图。对于测试发现的缺陷，按严重程度分级（致命缺陷/严重缺陷/一般缺陷/轻微缺陷）：

◦ 致命缺陷：核心功能无法使用（如无法提交申请、审批流程中断），需立即修复；

◦ 严重缺陷：功能实现不符合需求，但存在替代方案，需 24 小时内修复；

◦ 一般缺陷：不影响核心流程的功能瑕疵（如界面显示错位），需在测试周期内修复；

◦ 轻微缺陷：优化类问题（如操作提示不够清晰），可根据优先级择期修复。

实施团队建立缺陷跟踪台账，记录缺陷描述、严重程度、发现人、发现时间、修复人、修复时间、回归测试结果，确保所有缺陷闭环管理，修复后的功能需重新进行回归测试，验证无衍生问题。

9.1.5.2 性能测试

性能测试旨在验证系统在预期业务负载下的响应速度、并发处理能力、稳定性，确保系统满足部署单位的实际业务运行需求，测试工具采用 JMeter、LoadRunner 等专业性能测试工具。

• 测试场景与指标定义：

◦ 并发用户测试：模拟不同并发用户数（如 100 人、300 人、500 人、1000 人）同时登录系统、提交用章申请、处理审批、上传文件，测试系统的并发处理能力，核心指标包括：平均响应时间（页面响应≤500ms，接口响应≤300ms）、并发用户数阈值（支持≥500 并发用户正常操作）、事务成功率（≥99.9%）。

◦ 压力测试：在并发用户数逐步增加（从 500 人增至 2000 人）的情况下，测试系统的极限承载能力，观察系统是否出现卡顿、崩溃、数据丢失等问题，记录系统的最大并发承载量、CPU 使用率（峰值≤80%）、内存使用率（峰值≤85%）、数据库连接池使用率（峰值≤90%）等指标。

◦ 稳定性测试：模拟正常业务负载（300 并发用户），持续运行 72 小时，测试系统的长期稳定性，核心指标包括：系统无崩溃、无内存泄漏（内存使用率稳定在合理范围）、事务成功率保

持≥99.9%、日志记录完整无丢失。

◦ 大数据量测试：在数据库中导入 10 万条历史审批记录、1 万份上传文件，测试系统的查询性能（列表查询≤1 秒，精准查询≤300ms）、文件上传/下载（仅测试上传，V1.0 未启用下载）速度（单文件上传≤1.5 秒）、报表生成效率（统计报表生成≤3 秒）。

• 测试结果分析与优化：
性能测试完成后，实施团队分析测试报告，识别系统性能瓶颈（如数据库查询慢、服务器资源不足、代码逻辑冗余等），并进行针对性优化：

◦ 数据库优化：添加索引、优化 SQL 语句、调整数据库连接池参数；

◦ 服务器优化：增加 CPU/内存资源、优化 Web 服务器配置（如 Nginx 的并发连接数）；

◦ 代码优化：简化复杂业务逻辑、优化文件上传/处理流程、启用缓存机制（如 Redis 缓存常用数据）。

优化后重新进行性能测试，确保系统性能指标达到预设标准。

9.1.5.3 安全测试

安全测试旨在发现系统潜在的安全漏洞，防范黑客攻击、数据泄露等风险，测试内容覆盖身份认证、权限控制、数据安全、代码安全等维度，可结合人工渗透测试与自动化工具测试（如 OWASP ZAP、Nessus）。

• 核心测试项目：

◦ 身份认证安全：测试弱口令（如 123456、admin@123）能否通过、密码哈希值是否可逆、登录失败锁定机制是否生效、会话标识是否可预测、是否存在会话劫持风险。

◦ 权限控制安全：测试普通用户能否越权访问审批端/管理端功能、审批人能否审批自身提交的申请、低权限用户能否查看/修改高权限用户的数据、文件上传是否存在越权访问（如访问其他用户上传的文件）。

◦ 数据安全：测试敏感数据（如手机号、审批意见）传输是否加密、存储是否加密、数据库是否存在 SQL 注入漏洞（通过输入特

殊字符测试)、文件上传是否存在恶意文件上传漏洞（如上传可执行脚本文件)。

◦ 日志安全：测试能否修改/删除系统日志、日志导出是否需要权限校验、日志记录是否完整（如操作人、时间、IP 是否准确)。

◦ 其他安全测试：测试服务器端口是否开放过多、是否存在敏感文件泄露（如配置文件、源代码)、是否存在跨站脚本攻击（XSS）漏洞。

• 安全整改与验证：
对于安全测试发现的漏洞，实施团队按漏洞风险等级（高危/中危/低危）制定整改计划，高危漏洞（如 SQL 注入、越权访问）需立即修复，中危漏洞需在测试周期内修复，低危漏洞可择期优化。整改完成后，进行安全回归测试，确保漏洞已彻底修复，无衍生安全问题。建议部署单位邀请第三方安全机构进行独立安全评估，出具安全测评报告，作为系统上线的重要依据。

9.1.5.4 兼容性测试

兼容性测试旨在验证系统在不同运行环境下的正常使用能力，确

保覆盖部署单位的实际使用场景：

• 浏览器兼容性：测试系统在主流浏览器（Chrome 90+、Firefox 88+、Edge 90+、Safari 14+）的运行情况，包括页面显示、功能操作、文件上传等，确保无界面错乱、功能失效等问题。

• 移动端兼容性：测试系统在 iOS、Android 系统的主流手机浏览器（如微信浏览器、手机 Chrome）中的使用情况，确保核心功能（申请提交、审批处理、文件上传）可正常操作，页面适配移动端屏幕。

• 操作系统兼容性：测试系统在推荐的 Linux 发行版（CentOS 7.9、Ubuntu 20.04）及 Windows Server 2019（可选部署环境）中的运行稳定性，验证数据库、中间件与操作系统的兼容性。

9.1.5.5 测试报告编制

测试验证阶段完成后，实施团队编制《系统测试报告》，内容包括：测试概述（测试目的、范围、环境、工具）、功能测试结果（用例执行情况、缺陷统计与闭环情况）、性能测试结果（各场景

测试指标、优化措施）、安全测试结果（漏洞统计、整改情况）、兼容性测试结果、测试结论（系统是否满足上线要求）。《系统测试报告》经测试小组各方签字确认后，作为系统验收的核心依据。

9.1.6 培训赋能阶段

培训赋能是确保部署单位用户能够熟练使用系统的关键，实施团队根据用户角色（管理员、审批人、普通用户、盖章员）制定差异化培训方案，采用“理论讲解+实操演示+现场答疑”的方式开展培训，确保每位用户掌握对应角色的核心操作。

9.1.6.1 培训对象与内容

- 管理员培训（1-2 天，线下/远程）：

培训对象为部署单位的系统管理员、IT 负责人，培训内容包括：系统架构与核心原理、管理端功能操作（账号管理、角色权限配置、组织架构维护、审批流程设计、编号规则配置、系统参数设置、日志查询与导出）、安全配置（HTTPS 配置、密码策略设置、文件权限管理）、日常运维操作（服务启停、日志查看、常见问题排查）、数据备份与恢复流程。培训后提供《管理员操作手册》，组织实操考核，确保管理员具备独立维护系统的能

力。

• 审批人培训（0.5 天，线下/远程）：
培训对象为各部门审批员，培训内容包括：系统登录、待办审批查看、审批详情查阅（申请信息、上传文件）、审批通过/驳回操作、审批记录查询与导出、常见问题处理（如驳回意见填写、申请材料补充要求）。培训后组织实操演练，确保审批人能够高效处理审批任务。

• 普通用户培训（0.5 天，可分部门开展）：
培训对象为发起用章申请的员工，培训内容包括：系统登录、初始密码修改、用章申请提交（表单填写、文件上传）、申请状态查询、撤回申请操作、常见问题咨询渠道。培训后提供《普通用户操作手册》，确保用户能够独立发起用章申请。

• 盖章员培训（0.5 天，线下）：
培训对象为负责线下盖章的工作人员，培训内容包括：系统登录、待盖章申请查看、盖章文件上传（与审批记录绑定）、盖章记录查询、文件上传校验规则。培训后组织实操演练，确保盖章员能够准确上传盖章文件，完成归档操作。

9.1.6.2 培训材料与形式

• 培训材料：提供纸质版/电子版《操作手册》（按角色划分）、培训 PPT、操作演示视频，便于用户课后复习。

• 培训形式：优先采用线下集中培训，对于跨区域用户可采用远程视频培训；实操环节安排讲师现场指导，及时解答用户疑问；培训结束后收集用户反馈，针对共性问题开展补充培训。

9.1.7 验收上线阶段

验收上线阶段是系统实施的收尾环节，部署单位根据《需求确认说明书》《系统测试报告》《培训记录》等文件，对系统进行全面验收，确认系统满足业务需求后，正式上线运行。

9.1.7.1 验收流程

• 验收准备：实施团队整理验收材料，包括《需求确认说明书》《环境验收报告》《系统安装报告》《数据迁移报告》《系统测试报告》《培训记录》《操作手册》、交付物清单等，提交部署单位。

• 现场验收：部署单位组织业务骨干、IT 部门、安全部门组成验收小组，进行现场验收：① 功能验证：随机抽取核心功能

（如申请提交、审批处理、日志查询）进行实操验证；② 性能验证：模拟实际业务场景，测试系统响应速度与稳定性；③ 安全验证：检查安全配置（如 HTTPS、密码策略、权限控制）是否生效；④ 交付物核对：核对交付物清单是否完整。

• 问题整改：若验收过程中发现问题，实施团队及时整改，整改完成后重新提交验收；若验收无异议，验收小组签署《系统验收单》，确认系统验收通过。

9.1.7.2 上线部署

• 上线策略：采用“灰度上线”模式，先在部分部门（如试点部门）上线运行 1-2 周，收集用户反馈，优化系统功能与操作流程，确保系统稳定后，再在全单位推广上线。

• 上线操作：实施团队协助部署单位进行上线配置，包括：① 最终数据备份（上线前对系统数据进行全量备份）；② 系统切换：将测试环境的配置同步至生产环境，启用正式账号；③ 通知发布：向全单位发布系统上线通知，明确上线时间、使用范围、操作指南、咨询渠道。

• 上线支持：上线后提供 7×24 小时故障响应支持，实施团队安

排专人负责处理用户反馈的问题，对于紧急问题（如系统无法访问、核心功能失效）1 小时内响应，4 小时内解决；对于一般问题 24 小时内解决。

9.2 交付物清单

为确保部署单位能够独立使用、维护系统，实施团队提供完整的标准化交付物，所有交付物经双方确认后移交，具体清单如下：

9.2.1 技术交付物

- 系统安装包：包括应用程序安装包、数据库初始化脚本、配置文件模板；

- 源代码相关：源代码清单（含版本号）、代码注释文档、编译脚本（若需要）；

- 数据库相关：数据库脚本（建库、建表、索引、存储过程）、数据字典（字段定义、表间关联、索引说明）、数据迁移脚本；

- 部署相关：《环境准备指南》《系统安装部署手册》《安全配置指南》《数据备份与恢复手册》。

9.2.2 文档交付物

• 需求与设计文档：《需求确认说明书》《系统架构设计说明书》《功能模块设计文档》《数据库设计说明书》；

• 测试与验收文档：《测试用例集》《系统测试报告》《安全测评报告》（若第三方检测）《环境验收报告》《数据迁移报告》《系统验收单》；

• 操作与运维文档：《管理员操作手册》《普通用户操作手册》《审批人操作手册》《盖章员操作手册》《日常运维规范》《常见问题排查指南》；

• 其他文档：《培训 PPT》《操作演示视频》《交付物清单》《培训记录》。

9.2.3 其他交付物

• 账号信息：系统超级管理员账号、各部门管理员账号、初始测试账号（含密码），以加密文档形式移交；

• 软件著作权相关：若需申请软件著作权，提供《系统功能说明》《系统架构图》《核心代码片段》《数据字典》等申报材料；

• 售后支持信息：售后联系人、联系方式、支持期限、响应流程。

所有交付物采用电子文档（加密压缩包）+ 纸质文档（关键文档签字版）的形式移交，电子文档存储在移动硬盘或光盘中，纸质文档经双方签字确认后归档留存。

9.3 培训与上线支持

实施团队提供全周期培训与上线支持服务，确保部署单位用户快速上手、系统稳定运行，具体服务内容如下：

9.3.1 培训服务

• 定制化培训方案：根据部署单位的用户规模、角色分布、业务需求，制定个性化培训计划，灵活调整培训时间、形式、内容；

• 多层级培训实施：按管理员、审批人、普通用户、盖章员分层开展培训，确保不同角色掌握对应操作技能；

• 课后辅导支持：培训结束后 1 个月内，提供线上课后辅导（如微信群、远程协助），解答用户在实际使用中遇到的问题；

• 培训效果评估：通过实操考核、问卷调查等方式，评估培训效果，针对薄弱环节开展补充培训。

9.3.2 上线支持服务

• 支持期限：提供上线后 3 个月的免费支持服务（可根据合同约定延长），包括故障排查、问题修复、功能优化建议；

• 故障响应机制：建立分级响应机制，紧急故障（系统崩溃、数据丢失）1 小时内响应，4 小时内解决；重要故障（核心功能异常）2 小时内响应，8 小时内解决；一般故障（界面显示问题、操作疑问）24 小时内响应并解决；

• 定期巡检服务：上线后每月进行 1 次系统巡检，检查系统运行状态、数据库性能、安全配置，出具《巡检报告》，提出优化建议；

• 需求收集与反馈：收集部署单位的功能优化建议，整理后形成

《需求反馈报告》，为系统后续版本升级提供参考。

9.3.3 长期服务保障

为确保系统长期稳定运行，匹配部署单位业务发展与合规要求的动态变化，实施团队建立全生命周期长期服务保障体系，提供持续化、专业化的技术支持与升级服务，具体内容如下：

9.3.3.1 版本迭代与升级支持

系统将根据行业技术发展、政策合规更新（如等保标准升级、个人信息保护法规修订）及用户反馈的共性需求，持续进行版本迭代优化。部署单位可享受以下升级相关服务：

- 升级规划咨询：新版本发布后，第一时间向部署单位推送版本说明，详细列明新增功能模块、现有功能优化点、安全补丁清单及兼容性说明。实施团队将结合部署单位的业务场景、现有系统配置及未来发展规划，提供定制化升级建议，明确升级范围、预期业务价值、实施周期、资源需求及潜在风险点，协助部署单位决策是否升级及升级时机。

- 升级实施服务：若部署单位确认升级，实施团队将提供全流程

闭环升级支持。升级前，完成系统全量数据备份（含数据库数据、上传文件、配置文件），并在测试环境进行预升级验证，模拟生产环境场景测试升级后功能稳定性、数据一致性及与第三方系统的兼容性；升级中，采用灰度升级策略，先在非核心业务节点或部分部门试点升级，验证无问题后再全面推广，避免升级过程影响整体业务运行；升级后，开展功能抽检、数据校验及性能测试，确保升级后系统运行正常，数据无丢失、无错乱，同时提供升级总结报告，列明升级内容、实施过程及后续注意事项。

• 兼容适配保障：针对部署单位已对接的第三方系统（如 OA 系统、档案管理系统、SSO 单点登录系统），升级前将进行专项兼容性测试，梳理接口适配需求。若因版本升级导致接口参数或数据格式变化，实施团队将提供接口适配改造服务，编写适配脚本，协助部署单位完成第三方系统对接调整，确保升级后系统间数据流转顺畅、功能协同正常。

• 历史版本支持：对于暂不计划升级的部署单位，实施团队将提供至少 18 个月的历史版本安全支持，及时推送高危安全漏洞修复补丁，协助部署单位进行安全加固，保障历史版本系统的运行安全，同时定期提供版本安全风险评估报告，提醒潜在安全隐患及应对建议。

9.3.3.2 技术咨询与运维支持

支持期限结束后，部署单位可通过签订年度服务协议的方式，享受长期技术咨询与运维支持服务，确保系统日常运行问题得到及时响应与解决：

• 7×12 小时专属咨询通道：开通专属技术咨询热线、企业微信/钉钉服务群及邮件咨询渠道，由具备 3 年以上系统运维经验的资深工程师提供实时响应服务。针对系统运维、功能使用、权限配置、参数调整、故障排查等各类问题，提供电话指导、远程协助或文档支持，确保问题得到快速解答。

• 远程运维协助：针对复杂运维问题（如数据库性能下降、系统卡顿、数据异常、第三方接口对接故障等），技术工程师可通过授权远程登录方式，协助部署单位管理员定位问题根源，制定针对性解决方案并指导实施。如需现场支持，可根据合同约定安排工程师上门服务，现场排查并解决问题。

• 运维技能提升培训：每年提供 1-2 次免费运维技能提升培训，培训内容根据部署单位运维需求定制，包括数据库索引优化、SQL 语句调优、服务器资源监控、安全防护进阶、系统性能调优、故障应急处理等实战技能，培训形式采用线上直播+线下实

操结合，帮助部署单位管理员提升自主运维能力，减少对外部支持的依赖。

• 运维文档动态更新：根据系统版本升级、政策法规变化及运维实践经验，定期更新《日常运维规范》《常见问题排查指南》《应急处理流程》《数据备份与恢复操作手册》等文档，同步至部署单位并提供更新说明，确保运维人员使用的文档始终具备时效性与准确性。

9.3.3.3 合规与安全保障服务

为帮助部署单位持续满足监管要求，规避合规风险，实施团队提供长期合规与安全保障服务，确保系统运行符合相关法律法规及行业标准：

• 合规更新支持：当《网络安全法》《数据安全法》《个人信息保护法》等相关法律法规，或《网络安全等级保护基本要求》等国家标准发生修订时，第一时间提供合规解读报告，明确修订内容对系统的影响，梳理系统需调整的配置项、功能模块或数据处理流程。协助部署单位制定合规整改方案，包括功能改造、参数配置优化、管理制度完善等，确保系统持续符合合规要求。

• 定期安全评估：每年提供 1 次免费系统安全评估服务，采用自动化安全扫描工具（如 OWASP ZAP、Nessus）与人工渗透测试相结合的方式，全面排查系统潜在的安全漏洞（如 SQL 注入、XSS 跨站脚本、越权访问、文件上传漏洞等）。评估完成后，出具《安全评估报告》，详细列明漏洞位置、风险等级、可能造成的危害及具体整改建议，协助部署单位完成漏洞修复与系统安全加固。

• 应急响应支持：若发生安全事件（如数据泄露、黑客攻击、病毒感染、系统被入侵等），部署单位可启动紧急响应流程，实施团队将在 2 小时内启动应急预案，协助部署单位定位事件源头、隔离受影响的系统节点、阻断攻击路径，防止事件扩大。同时，提供技术支持帮助恢复系统正常运行，分析事件原因并出具安全事件分析报告，提出后续防范措施，协助部署单位完善安全管理制度，避免类似事件再次发生。

9.3.3.4 个性化需求定制服务

随着部署单位业务规模扩大、管理流程优化或新业务场景出现，若产生个性化功能需求（如新增审批节点、扩展表单字段、新增统计报表、对接新的第三方系统等），实施团队提供定制化开发服务，满足部署单位差异化需求：

• 需求调研与方案设计：安排专业需求分析师与部署单位业务骨干、技术负责人深度对接，通过现场访谈、需求研讨会、场景模拟等方式，全面梳理需求细节、业务逻辑、输入输出要求及预期目标。基于调研结果，编制《个性化需求设计方案》，明确技术实现路径、开发周期、人力成本、质量标准及验收指标，方案经双方确认后启动开发工作。

• 定制开发与测试：组建专项开发团队，基于系统现有技术架构进行模块化开发，确保定制功能与原有系统架构兼容、代码风格统一，避免影响原有功能稳定性。开发过程中，定期向部署单位同步开发进度，提供阶段性成果演示，收集反馈并及时调整。开发完成后，进行全面的功能测试、性能测试、安全测试及兼容性测试，出具《定制开发测试报告》，确保定制功能满足需求且无衍生问题。

• 部署上线与培训：完成定制功能的部署上线，更新系统操作手册、管理员手册等相关文档。针对定制功能组织专项培训，覆盖相关用户角色，通过理论讲解、实操演示、案例分析等方式，确保用户掌握新功能的使用方法。上线后提供 1 个月的专项支持，及时解决用户使用过程中遇到的问题，确保定制功能顺利落地应用。

十、测试与验收

测试与验收是保障系统质量、确保系统满足部署单位业务需求与合规要求的关键环节，本章节明确测试的核心类型、执行标准及验收流程与依据，确保测试全面覆盖、验收客观公正，为系统正式上线提供坚实保障。

10.1 功能测试

功能测试是验证系统核心业务流程与功能模块是否符合《需求确认说明书》要求的基础测试，旨在确保系统所有已规划功能均已实现，且操作流程顺畅、数据处理准确。

10.1.1 测试范围与核心内容

功能测试覆盖系统全模块、全流程，无遗漏核心功能点，具体核心测试内容包括：

• 账号与权限管理：验证账号创建、编辑、启用/禁用、密码修改、角色分配、权限继承等操作的准确性；测试权限校验机制，确保不同角色用户仅能访问授权功能模块与数据；验证登录失败

锁定机制（达到阈值后账号锁定）、历史登录记录查询功能的完整性与准确性。

• 登录功能：测试用户名/密码登录的正常流程与异常场景（账号不存在、密码错误、账号锁定）；验证会话管理功能（会话超时自动退出、同一账号多设备登录限制）；校验 HTTPS 协议适配效果，确保登录过程数据传输加密；检查登录日志记录的字段完整性（用户名、登录时间、IP 地址等）。

• 用章申请提交：测试表单字段校验逻辑，包括必填字段校验（未填写时无法提交）、格式校验（手机号、日期等符合规范）、业务规则校验（所属部门与申请人权限匹配）；验证文件上传功能，支持的文件格式、大小限制、上传数量限制是否符合配置要求；测试申请提交、撤回、修改、状态查询等操作的正常性，确保申请状态流转准确。

• 审批管理：验证待办审批推送的及时性（申请提交后审批端实时接收）；测试审批详情查看功能，确保申请信息、上传文件元数据、历史操作记录完整展示；校验审批通过/驳回操作的有效性，驳回意见必填校验机制（未填写驳回意见无法提交）；测试审批编号自动生成的唯一性与格式正确性；验证审批记录查询与检索功能（按编号、部门、时间等维度），审批链追溯的完整

性。

• 盖章文件上传：测试盖章文件与审批记录的绑定逻辑，确保文件上传后准确关联对应申请；验证文件上传校验机制（格式、大小限制）；检查申请状态更新准确性（上传盖章文件后从“待盖章”变为“已归档”）；校验上传日志记录的完整性（上传人、上传时间、文件信息等）。

• 日志与审计：测试登录日志、操作日志、系统日志、安全日志的记录完整性，确保所有关键操作均有日志留存；验证日志查询功能（多条件组合筛选）、导出功能（支持 CSV/Excel 格式）的正常性；测试日志不可篡改性，确保已生成日志无法修改或删除。

• 管理端配置：验证组织架构维护（新增、编辑、删除部门）、角色权限配置（权限项勾选、角色分配）的即时生效性；测试审批流程设计功能（新增审批节点、调整审批顺序）、编号规则修改（前缀、流水位数等参数调整）的有效性；校验系统参数设置（文件上传大小、日志留存期限）、日志导出权限控制的合理性。

• 异常场景处理：测试网络中断、文件上传失败、数据库连接异常、并发操作冲突等异常场景下，系统的容错能力（无崩溃、无

死锁)；验证错误提示的清晰度与引导性（明确告知用户错误原因及解决方法)；测试异常恢复后的数据一致性（如网络恢复后未完成的申请可继续提交，数据无丢失)。

10.1.2 测试执行标准

功能测试需严格遵循以下执行标准，确保测试结果客观有效：

• 测试用例覆盖率：核心功能测试用例覆盖率达到100%，边缘场景、异常场景测试用例覆盖率不低于95%，无遗漏关键业务流程与操作场景。

• 功能实现一致性：所有功能的实现效果与《需求确认说明书》描述完全一致，无功能缺失、功能冗余或功能偏离需求的情况。

• 数据处理准确性：表单提交、审批操作、文件上传、日志记录等环节的相关数据（如申请信息、审批意见、文件元数据、时间戳、审批编号）准确无误，无数据丢失、错乱、重复或格式错误。

• 操作流程顺畅性：各功能模块的操作流程符合业务逻辑与用户使用习惯，操作步骤简洁合理，无流程阻塞、步骤冗余或逻辑矛

盾的情况，用户无需专业培训即可快速上手。

• 异常处理合理性：系统在异常场景下无崩溃、无死锁，错误提示清晰明确，能够引导用户正确处理异常；异常恢复后，系统状态与数据保持一致，不影响后续业务操作。

10.1.3 缺陷判定与整改标准

根据缺陷对系统运行的影响程度，划分为四个等级，明确整改要求：

• 致命缺陷：核心业务流程无法运行（如无法提交申请、审批操作无效、系统频繁崩溃）、数据严重错乱或丢失，此类缺陷需立即修复，修复后需重新进行全流程回归测试，确保无衍生问题。

• 严重缺陷：功能实现不符合需求，但存在替代操作方案（如审批记录导出格式不符合要求，但可通过其他方式转换），此类缺陷需在 24 小时内修复，修复后进行相关模块回归测试。

• 一般缺陷：不影响核心流程的功能瑕疵（如界面显示错位、操作提示文字不规范、非关键字段校验逻辑不完善），此类缺陷需在测试周期内修复，修复后进行单点回归测试。

• 轻微缺陷：优化类问题（如操作步骤可简化、界面美观度提升、日志导出速度可优化），此类缺陷可根据项目优先级择期修复，不影响系统整体验收。

10.2 性能测试

性能测试旨在验证系统在预期业务负载与极限压力下的运行稳定性、响应速度与并发处理能力，确保系统能够满足部署单位日常业务运行及峰值场景需求。

10.2.1 测试类型与核心场景

性能测试涵盖并发测试、压力测试、稳定性测试、大数据量测试、峰值场景测试五大类型，核心测试场景如下：

• 并发测试：模拟多用户同时进行核心操作，包括 100 人、300 人、500 人、1000 人并发登录系统、提交用章申请、处理审批任务、上传盖章文件，测试系统在不同并发量级下的处理能力。

• 压力测试：逐步增加并发用户数（从 500 人逐步增至 2000 人），持续加压至系统出现性能瓶颈（如响应时间显著延长、事

务失败率上升），测试系统的极限承载能力，观察系统在高负载下的运行状态（是否崩溃、是否出现数据丢失）。

• 稳定性测试：模拟正常业务负载（300 并发用户），持续运行 72 小时，期间定期执行核心操作（申请提交、审批处理、查询统计），测试系统的长期稳定运行能力，观察系统资源占用变化（CPU、内存使用率是否稳定）。

• 大数据量测试：在数据库中导入 10 万条历史审批记录、1 万份各类格式的上传文件（含图片、文档），测试系统的查询性能（列表分页查询、多条件精准查询）、统计报表生成效率、文件归档与检索速度。

• 峰值场景测试：模拟业务高峰期（如月末、年末用章申请集中提交），在 1 小时内集中发起 5000 条用章申请，测试系统在短时间内大量申请提交、审批处理的响应速度与处理效率，确保无申请拥堵、处理超时情况。

10.2.2 性能指标基准

性能测试需达到以下明确指标基准，确保系统满足实际业务需求：

• 页面响应时间：普通页面（如登录页、首页、申请列表页）响应时间不超过 500 毫秒，复杂页面（如审批详情页、包含大数据量的统计报表页）响应时间不超过 800 毫秒，从页面发起请求到完全加载完成的时间需符合该标准。

• 接口响应时间：普通接口（如用户登录、申请状态查询）响应时间不超过 300 毫秒，复杂接口（如大数据量查询、审批流程提交）响应时间不超过 1 秒，从接口接收请求到返回完整响应结果的时间需满足该要求。

• 并发用户承载量：系统支持不少于 500 并发用户同时进行核心操作，操作过程无卡顿、无超时提示，事务处理正常。

• 事务成功率：所有业务事务（申请提交、审批处理、文件上传等）的成功率不低于 99.9%，即成功完成的业务事务数与总事务数的比值不低于 99.9%。

• CPU 使用率：服务器 CPU 在高负载场景下（如 1000 人并发操作）的峰值使用率不超过 80%，避免 CPU 资源耗尽导致系统响应缓慢。

• 内存使用率：服务器内存在高负载场景下的峰值使用率不超过85%，无内存泄漏情况（持续运行期间内存使用率无持续上升趋势）。

• 数据库 TPS：数据库每秒处理的事务数不低于 1000，确保数据库能够高效处理系统产生的业务请求。

• 单文件上传速度：200MB 以内的文件上传速度不超过 1.5 秒，从文件开始上传到系统确认存储完成的时间需符合该标准。

• 大数据量查询速度：包含 10 万条记录的列表查询响应时间不超过 1 秒，精准查询（按审批编号、申请人等条件）响应时间不超过 300 毫秒。

10.2.3 性能优化与复测要求

• 性能瓶颈整改：若测试发现某一性能指标未达基准要求，实施团队需深入分析瓶颈原因，可能的原因包括数据库索引缺失、SQL 语句逻辑冗余、服务器资源配置不足、代码执行效率低、缓存机制未合理利用等。针对具体原因制定针对性优化方案，如添加数据库索引、优化 SQL 语句、调整服务器配置（增加 CPU/内存）、优化代码逻辑、启用 Redis 缓存等。

• 优化后复测：优化方案实施完成后，需对相关性能场景进行复测，确保所有性能指标均达到基准要求，且无新的性能问题产生。若优化后仍未达标，需重新分析原因并调整优化方案，直至指标符合要求。

• 性能报告编制：性能测试完成后，编制《性能测试报告》，详细记录测试环境（硬件配置、软件版本、网络环境）、测试场景设计、测试数据（并发用户数、事务数、响应时间）、指标结果（是否达标）、性能瓶颈分析、优化措施及复测情况，作为系统性能达标与否的核心依据。

10.3 安全测试

安全测试旨在全面排查系统潜在的安全漏洞与风险点，验证系统的安全防护措施是否有效，确保系统满足等保二级及相关安全标准要求，防范数据泄露、黑客攻击等安全事件，为系统长期安全运行筑牢防线。

10.3.1 测试范围与核心项目

安全测试覆盖系统全链路安全防护环节，从身份认证到数据存

储、从代码实现到网络部署，无遗漏关键安全节点，核心测试项目如下：

• 身份认证安全：开展弱口令检测，测试是否存在简单密码（如123456、admin@123、用户名+123 等）可登录的情况，验证系统密码复杂度校验机制是否生效；检查密码存储安全性，确认是否采用不可逆哈希算法（如 SHA-256）加密存储，无明文或可逆加密存储情况；测试登录失败锁定机制，验证连续输入错误密码达到配置阈值（默认 5 次）后，账号是否自动锁定，锁定时长是否符合配置要求，且锁定事件是否完整记录；校验会话管理安全性，包括会话标识（Session ID）是否采用随机高强度字符串生成、是否可预测或篡改，会话超时控制是否有效（默认 2 小时无操作自动退出），同一账号多设备登录是否存在权限冲突或会话劫持风险。

• 权限控制安全：执行越权访问测试，包括横向越权（普通用户能否访问其他用户的申请记录、文件数据）和纵向越权（低权限用户能否访问审批端/管理端功能模块、高权限操作），验证权限校验机制是否在接口层、业务层双重生效；检查权限分配合理性，确保基于角色的权限分配符合最小权限原则，无冗余权限或超范围授权情况；测试敏感操作权限校验，如日志导出、账号删除、系统配置修改等关键操作，是否仅允许授权管理员执行；验

证文件访问权限控制，确保用户仅能访问自身提交或关联的文件，无法通过URL拼接、路径遍历等方式访问其他用户上传的文件或系统敏感文件。

• 数据安全：开展SQL注入漏洞测试，在表单输入框、接口参数中注入特殊SQL语句（如UNION查询、报错注入语句），验证系统是否存在SQL注入风险，输入数据是否经过过滤、转义处理；测试敏感数据传输加密，通过抓包工具捕获用户登录、申请提交等环节的网络传输数据，验证是否通过HTTPS协议（TLS 1.2及以上版本）加密传输，无明文传输敏感信息（如密码、手机号、审批意见）的情况；检查敏感数据存储加密，确认手机号、身份证号（若有）等敏感字段是否采用字段级加密存储，加密密钥是否安全保管；执行文件上传漏洞测试，尝试上传可执行脚本文件（如.php、.asp文件）、恶意程序、伪装格式的危险文件（如将.exe文件改为.jpg后缀），验证系统是否对文件类型、后缀名、文件内容进行双重校验，是否存在恶意文件上传风险。

• 代码安全：进行跨站脚本攻击（XSS）漏洞测试，在表单输入框、评论区等位置注入恶意JavaScript代码，验证系统是否对输入内容进行过滤、编码处理，是否存在存储型XSS或反射型XSS漏洞；测试跨站请求伪造（CSRF）漏洞，构造恶意请求链接或页面，验证系统是否通过Token验证、Referer校验等方式防

范 CSRF 攻击；开展敏感信息泄露测试，检查系统错误提示（如数据库连接失败、权限不足时）是否泄露敏感信息（如数据库地址、表名、账号信息），配置文件、日志文件是否存在泄露风险，源代码是否有注释泄露敏感逻辑。

• 日志安全：验证日志记录完整性，检查所有关键操作（登录、申请提交、审批处理、权限变更、文件上传、日志导出）是否均生成日志，日志字段是否包含操作人、操作时间、操作 IP、操作类型、操作结果等核心信息；执行日志防篡改测试，尝试通过数据库操作、文件编辑等方式修改已生成的日志记录，验证日志是否采用追加写入、只读保护等机制，无法修改或删除；测试日志导出权限控制，确保仅具备审计权限的管理员可导出日志，导出操作是否生成审计记录，日志导出文件是否有访问权限限制。

• 服务器与网络安全：检查服务器端口开放情况，验证是否仅开放系统必需的端口（如 80 端口、443 端口、3306 端口），无不必要端口（如 FTP 端口、Telnet 端口）开放；测试防火墙规则有效性，验证是否仅允许授权 IP 地址访问服务器，是否能有效拦截恶意 IP 的攻击请求；检查服务器账号权限合理性，确保系统运行使用专用服务账号，无管理员权限，禁用默认账号、冗余账号；验证服务器防病毒软件适配性，检查防病毒软件是否正常运行，病毒库是否及时更新，能否检测到恶意文件或病毒。

10.3.2 安全测试标准

安全测试需严格遵循以下标准，确保系统达到既定安全等级要求：

- 高危漏洞零容忍：不允许存在任何高危安全漏洞，包括但不限于 SQL 注入、越权访问、恶意文件上传、XSS 跨站脚本攻击、会话劫持等可直接导致数据泄露、系统被控制的漏洞，发现后需立即启动紧急修复流程，修复后进行专项复测，确保漏洞彻底消除。

- 中危漏洞严格管控：中危安全漏洞（如弱口令策略未强制生效、日志字段缺失敏感信息、部分接口未做 CSRF 防护等）数量不得超过 3 个，且需在测试周期内完成修复，修复后进行相关模块的回归测试，验证漏洞已修复且无衍生安全问题。

- 低危漏洞明确处置：低危安全漏洞（如错误提示不够规范、部分非核心接口未做数据过滤、界面存在隐藏调试入口等）需逐一梳理，提供明确的整改计划或风险规避措施，若暂不修复需评估潜在风险，确保不影响系统核心安全与正常运行，且不违反相关合规要求。

• 合规性达标要求：安全测试结果需全面满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）二级等级保护的安全技术要求，符合《网络安全法》《数据安全法》《个人信息保护法》对数据安全与个人信息保护的相关规定，无合规性问题。

10.3.3 第三方安全评估（可选）

对于政府机关、国有企业、金融机构等安全要求较高的部署单位，建议委托具备国家认可资质的第三方安全评估机构（如具备《网络安全等级测评与检测评估机构服务认证证书》的机构）对系统进行独立安全测评。第三方机构将按照等保二级测评标准及相关安全规范，采用专业工具扫描、人工渗透测试、安全配置核查等多种方式，开展全面安全评估，出具具有法律效力的《安全测评报告》。

第三方测评结果将作为系统安全验收的核心依据，若测评发现安全问题，实施团队需根据测评报告中的整改建议，制定详细的整改方案，限期完成漏洞修复与安全加固，并配合第三方机构进行复测，直至系统通过第三方安全评估，确保系统安全防护能力达到行业领先水平。

10.4 兼容性测试

兼容性测试旨在验证系统在不同运行环境下的适配能力，确保系统能够满足部署单位多样化的使用场景，无界面错乱、功能失效等问题，提升用户使用体验。

10.4.1 测试范围与核心场景

兼容性测试覆盖浏览器、移动端、操作系统、硬件设备四大维度，核心测试场景如下：

• 浏览器兼容性：测试主流浏览器的最新版本及常用稳定版本，包括 Chrome 90 及以上版本、Firefox 88 及以上版本、Edge 90 及以上版本、Safari 14 及以上版本，验证系统在各浏览器中的页面显示（布局、字体、图片、按钮位置）是否正常，核心功能（登录、申请提交、审批处理、文件上传、日志查询）是否可正常操作，无样式错乱、功能卡顿或失效情况。

• 移动端兼容性：测试 iOS 14.0 及以上版本、Android 10.0 及以上版本的主流手机型号（如 iPhone 12 及以上系列、华为 Mate 40 及以上系列、小米 11 及以上系列、OPPO Find X3 及以

上系列），验证系统在手机自带浏览器、微信浏览器、手机Chrome等常用移动端浏览器中的适配效果，核心功能（申请提交、审批处理、文件上传、状态查询）是否可正常使用，页面是否自适应移动端屏幕尺寸，无横向滚动、内容溢出或操作按钮不可点击的情况。

• 操作系统兼容性：测试系统在推荐部署环境及常见服务器操作系统中的运行稳定性，包括CentOS 7.9、Ubuntu 20.04、Windows Server 2019等，验证数据库（MySQL 5.7、MariaDB 10.5）、中间件（Nginx 1.20、Apache 2.4）与操作系统的兼容性，系统服务是否能正常启动、运行，核心功能是否无异常。

• 硬件设备兼容性：测试系统在不同配置的服务器硬件环境中的运行情况，包括单机部署（4核CPU、8GB内存、1TB SSD）、主备部署（两台同配置服务器）、集群部署（4台及以上服务器组成集群），验证不同硬件配置下系统的性能表现、稳定性，是否支持负载均衡、故障自动切换等功能，硬件资源占用是否在合理范围。

10.4.2 兼容性测试标准

兼容性测试需达到以下标准，确保系统在多样化环境中稳定运

行：

• 功能正常性：在所有测试环境下，系统核心功能（登录、申请提交、审批处理、文件上传、查询统计、日志导出）均可正常使用，无功能失效、操作卡顿、数据传输异常等问题，业务流程可完整闭环。

• 界面适配性：页面布局、字体大小、图片显示、按钮位置等在不同浏览器、不同屏幕尺寸下均保持一致且美观，无样式错乱、内容重叠、文字截断或空白过大等情况，移动端页面自适应效果良好，操作便捷。

• 交互流畅性：用户在不同环境下操作系统时，无点击无响应、输入延迟、页面加载缓慢等问题，交互反馈及时，操作体验一致，无因环境差异导致的使用障碍。

• 稳定性要求：在各测试环境下，系统持续运行 24 小时无崩溃、无死锁，无内存泄漏、资源耗尽等情况，核心功能运行稳定，数据处理准确。

10.5 验收流程与标准

10.5.1 验收流程

系统验收遵循“资料准备→现场验收→问题整改→最终确认”的闭环流程，确保验收工作有序、全面：

• 验收资料准备：实施团队整理完整的验收资料，包括《需求确认说明书》《系统测试报告》（含功能、性能、安全、兼容性测试结果）、《环境验收报告》《数据迁移报告》（若有）、《培训记录》《操作手册》《交付物清单》等，提交部署单位验收小组审核。

• 现场验收实施：部署单位组织业务骨干、IT 部门、安全部门组成验收小组，结合验收资料开展现场验收。验收小组通过实操验证（随机抽取核心功能进行操作）、数据核查（比对系统数据与原始数据一致性）、性能抽检（模拟并发场景测试响应速度）、安全核查（检查安全配置与漏洞整改情况）等方式，全面评估系统是否满足需求。

• 问题整改与复验：若验收过程中发现问题，验收小组出具《验收问题清单》，明确问题描述、严重程度、整改要求。实施团队在规定期限内完成问题整改，提交整改报告及复验申请。验收小组对整改情况进行复验，直至所有问题整改完成。

• 验收确认：验收无异议后，验收小组签署《系统验收单》，明确验收通过结论，系统正式交付部署单位使用。

10.5.2 验收核心标准

系统验收需满足以下核心标准，方可判定为验收通过：

• 功能达标：所有核心功能均已实现，与《需求确认说明书》描述一致，无功能缺失或偏离，缺陷整改率 100%（致命、严重、一般缺陷全部修复，轻微缺陷已明确处置方案）。

• 性能达标：性能测试各项指标（页面响应时间、接口响应时间、并发承载量、事务成功率等）均达到预设基准要求，系统在预期业务负载下运行稳定。

• 安全达标：无高危安全漏洞，中危漏洞整改完成，安全配置符合等保二级要求，通过内部安全测试或第三方安全评估。

• 兼容性达标：系统在规定的浏览器、移动端、操作系统、硬件环境中均可正常运行，无兼容性问题。

• 交付完整：交付物清单中的所有物品（技术交付物、文档交付

物、账号信息等）均已齐全、有效，满足部署单位后续使用与维护需求。

• 培训到位：相关用户（管理员、审批人、普通用户、盖章员）已完成培训，能够熟练掌握对应角色的操作技能，培训记录完整。

十一、部署与运维

部署与运维是确保系统长期稳定、安全运行的关键环节，本章节详细描述系统部署环境要求、安装初始化流程、日常运维规范、故障排查与恢复方案，为部署单位提供全面的运维指导。

11.1 部署环境要求

系统部署环境需满足硬件、软件、网络、安全四大维度的配置要求，确保系统运行稳定、性能达标、安全可控：

11.1.1 硬件环境要求

根据部署模式（单机/主备/集群）的不同，硬件配置要求如下：

• 单机部署（适用于用户规模≤500 人、日均申请量≤1000 条的场景）：

◦ 应用服务器：CPU≥4 核（推荐 8 核），内存≥8GB（推荐 16GB），存储≥1TB SSD（推荐 2TB，含系统文件、应用程序、上传文件存储），网卡≥1Gbps。

◦ 数据库服务器：CPU≥8 核（推荐 16 核），内存≥16GB（推荐 32GB），存储≥2TB SAS 硬盘（推荐 4TB，含数据库数据、日志存储），网卡≥1Gbps。

◦ 备份服务器：CPU≥4 核，内存≥8GB，存储≥2TB（与主服务器存储容量相当），用于数据备份与归档。

• 主备部署（适用于用户规模 500-1000 人、日均申请量 1000-3000 条的场景）：

◦ 主/备应用服务器：配置与单机部署应用服务器一致，两台服务器硬件配置相同。

◦ 主/备数据库服务器：配置与单机部署数据库服务器一致，支持数据库主从复制。

◦ 备份服务器：配置与单机部署备份服务器一致，支持异地备份。

• 集群部署（适用于用户规模≥1000 人、日均申请量≥3000 条的高并发场景）：

◦ 应用服务器：3 台及以上，每台配置 CPU≥8 核、内存≥16GB、存储≥1TB SSD、网卡≥1Gbps，支持负载均衡。

◦ 数据库服务器：3 台及以上，采用主从复制或集群架构（如 MySQL MGR），每台配置 CPU≥16 核、内存≥32GB、存储≥4TB SAS 硬盘。

◦ 备份服务器：2 台及以上，存储≥4TB，支持异地容灾备份。

◦ 负载均衡设备：支持 TCP/HTTP 协议转发，具备健康检查、故障自动切换功能。

◦ 分布式缓存服务器（可选）：Redis 集群，每台配置 CPU≥4 核、内存≥16GB，用于缓存常用数据，提升系统性能。

11.1.2 软件环境要求

• 操作系统：推荐 Linux 发行版（CentOS 7.9、Ubuntu 20.04），64 位系统，已完成安全加固（关闭不必要服务、禁用默认账号、修改默认端口）；若采用 Windows 服务器，推荐 Windows Server 2019，64 位系统。

• 中间件：Web 服务器推荐 Nginx 1.20 及以上版本或 Apache 2.4 及以上版本；PHP 运行环境推荐 PHP 8.0 及以上版本，需安装 GD 库、OpenSSL、PDO、Redis 扩展（若启用缓存）等必要组件。

• 数据库：推荐 MySQL 5.7 或 MariaDB 10.5 及以上版本，启用二进制日志、慢查询日志功能，配置数据库连接池参数（最大连接数≥1000）。

• 其他软件：防病毒软件（推荐企业级防病毒解决方案，如卡巴斯基、瑞星），日志分析工具（如 ELK Stack，可选），备份软件（支持自动备份、加密备份）。

11.1.3 网络环境要求

• 网络带宽：服务器所在网络带宽≥100Mbps，峰值带宽≥1Gbps，确保高并发场景下数据传输流畅。

• 网络延迟：服务器与客户端之间的网络延迟≤50ms，跨区域部署时需优化网络架构，降低延迟。

• 网络安全：配置防火墙、入侵防御系统（IPS）、入侵检测系统（IDS），开放系统必需端口（80、443、3306 等），关闭不必要端口；划分安全区域，将数据库服务器、应用服务器部署在内部局域网，与互联网隔离；远程运维需通过 VPN 接入，配置访问白名单。

11.1.4 安全环境要求

• 存储加密：服务器磁盘分区采用加密技术（如 Linux LVM 加密、Windows BitLocker），防止存储介质丢失导致数据泄露。

• SSL 证书：从权威 CA 机构申请合法的 SSL 证书，用于 HTTPS 协议配置，确保数据传输加密。

• 账号安全：服务器、数据库、中间件等均采用强密码策略，定期更换密码；禁用默认账号、冗余账号，为系统运行创建专用服

务账号，分配最小权限。

• 补丁管理：建立定期补丁更新机制，及时安装操作系统、中间件、数据库的安全补丁，修复已知漏洞。

11.2 安装与初始化步骤

系统安装与初始化遵循“环境检查→数据库部署→应用部署→参数配置→功能验证”的标准化流程，由实施团队主导实施，部署单位 IT 部门提供配合，确保安装过程规范、高效，初始化配置符合业务需求：

11.2.1 安装前环境检查

安装前需完成全面的环境检查，确保硬件、软件、网络、安全配置均满足系统运行要求，具体检查内容如下：

• 硬件配置检查：核实服务器 CPU、内存、存储、网卡等硬件参数是否符合部署模式对应的要求，检查存储设备是否正常挂载、磁盘空间是否充足（预留不少于 50%的冗余空间），确认服务器硬件无故障。

• 软件环境检查：验证操作系统版本（如 CentOS 7.9、Ubuntu 20.04）是否符合要求，已安装的中间件（Nginx/Apache）、PHP 版本、数据库版本是否达标；检查 PHP 必要扩展（GD 库、OpenSSL、PDO 等）是否安装并启用；确认服务器无端口冲突（80、443、3306 等系统必需端口未被其他服务占用）。

• 网络连通性检查：测试服务器与客户端、服务器之间的网络连通性，确保 ping 通、端口可访问；检查防火墙规则是否已配置，开放系统所需端口；验证服务器是否能正常访问外部资源（如 CA 证书下载、补丁更新）（若有需要）。

• 安全配置检查：确认服务器已完成安全加固（关闭不必要服务、禁用默认账号、修改默认端口）；检查防病毒软件是否安装并更新病毒库；核实存储加密、SSL 证书是否准备就绪。

环境检查完成后，填写《环境检查报告》，记录检查结果，若存在不符合项，由部署单位 IT 部门整改完成后再启动安装流程。

11.2.2 数据库部署与初始化

数据库部署是系统安装的核心环节，确保数据存储安全、访问高效，具体步骤如下：

• 数据库安装：根据选定的数据库类型（MySQL 5.7 或 MariaDB 10.5 及以上），在数据库服务器上执行安装程序，配置安装路径（建议独立分区存储）、数据存储路径、日志存储路径，设置数据库服务开机自启。

• 数据库安全配置：修改数据库默认管理员密码（采用强密码策略），禁用远程 root 登录权限；创建系统专用数据库账号，仅授予该账号对系统数据库的查询、插入、更新、删除权限，无数据库管理员权限；启用数据库二进制日志（用于数据恢复）、慢查询日志（用于性能优化），配置日志存储期限（默认不少于 30 天）；调整数据库核心参数，包括最大连接数（≥1000）、查询缓存大小、innodb 缓冲池大小（建议为服务器内存的 50%-70%）等，优化数据库性能。

• 数据库与表创建：执行系统提供的数据库初始化脚本，自动创建系统所需的数据库、数据表、索引、存储过程及触发器。脚本执行过程中，将自动创建用户表、部门表、角色表、审批表、文件表、日志表等核心数据表，并建立必要的主键、外键及索引（如审批编号唯一索引、用户 ID 索引），确保数据查询高效。

• 初始数据导入：导入系统基础配置数据，包括预设角色模板

（普通用户、审批员、盖章员、系统管理员）、默认系统参数（文件上传大小限制、密码策略、日志留存期限）、基础组织架构（如根部门）等，为系统运行提供基础数据支撑。

数据库部署完成后，测试数据库连接是否正常，执行基础查询语句验证数据表及数据是否创建成功，填写《数据库部署报告》。

11.2.3 应用程序部署

应用程序部署需确保程序文件完整、配置正确，与数据库正常联动，具体步骤如下：

• 程序文件上传：将系统安装包上传至应用服务器的指定目录（如/var/www/seal-system），解压安装包，确认程序文件（包括前端页面文件、后端逻辑文件、配置文件）完整无缺失。

• Web 服务器配置：在 Nginx 或 Apache 中配置虚拟主机，指定网站根目录（对应应用程序解压目录），配置端口（80 端口用于 HTTP，443 端口用于 HTTPS）；启用 PHP 解析功能，配置 PHP 运行参数（如内存限制≥512M、上传文件大小限制≥200M、执行时间限制≥30 秒）；配置 HTTPS 协议，导入 SSL 证书（公钥、私钥），强制所有访问通过 HTTPS 协议，禁用 HTTP 访问。

• 应用程序配置：修改应用程序核心配置文件（如config.php），配置数据库连接信息（数据库地址、端口、数据库名、用户名、密码），确保应用程序能正常连接数据库；配置文件存储路径（指定本地受控目录，如/data/seal-files）、日志存储路径（如/var/log/seal-system）；配置会话有效期（默认2小时）、缓存配置（若启用Redis缓存，需配置Redis服务器地址、端口、密码）。

• 文件权限设置：修改应用程序目录、文件存储目录、日志存储目录的访问权限，仅允许系统服务账号（如www-data）具备读写权限，其他账号无访问权限；确保上传文件目录仅允许应用程序写入，禁止执行权限，防范恶意文件执行风险。

应用程序部署完成后，启动Web服务与PHP服务，测试服务是否正常运行，无报错信息。

11.2.4 系统初始化配置

系统初始化配置需结合部署单位业务需求，完成组织架构、角色权限、审批流程等核心配置，具体步骤如下：

• 超级管理员账号创建：登录系统管理端初始登录入口，使用默认超级管理员账号（由实施团队提供）登录，首次登录后强制修改默认密码（符合密码策略），创建部署单位专属超级管理员账号，禁用默认初始账号。

• 组织架构配置：在管理端“组织架构管理”模块，创建部署单位的部门层级结构（如总部-分公司-部门-班组），填写部门名称、部门代号、负责人等信息，支持批量导入或手动添加，确保部门架构与实际业务一致。

• 角色与权限配置：基于预设角色模板，根据部署单位岗位职责，调整角色权限项（如新增“法务审批角色”，配置合同用章审批权限）；创建自定义角色（若有需要），勾选对应权限项，完成权限分配；将角色与部门关联，确保不同部门用户仅能获得本部门相关权限。

• 审批流程配置：在“审批流程管理”模块，创建不同用章类型的审批流程（如合同签署、公文用印、证明文件），配置审批节点（如部门负责人→法务→分管领导→盖章端），指定每个节点的审批人范围（如部门负责人为对应部门的管理员），设置审批规则（如紧急申请的审批时效、驳回后是否重新走全流程）。

• 系统参数配置：在“系统设置”模块，配置核心参数，包括审批编号生成规则（前缀、年份格式、部门代号、流水位数）、文件上传限制（单个文件大小、支持格式、单次上传数量）、密码策略（复杂度要求、有效期）、登录失败锁定阈值与锁定时长、日志留存期限、数据备份周期等，参数配置需符合部署单位管理要求。

初始化配置完成后，导出配置清单，由部署单位确认签字，作为后续系统维护的依据。

11.2.5 功能验证与安装收尾

安装与配置完成后，进行全面的功能验证，确保系统正常运行，具体步骤如下：

• 核心功能验证：创建测试用户账号（分配不同角色），测试登录、申请提交、审批处理、文件上传、日志查询、权限校验等核心功能，验证业务流程顺畅、数据处理准确。

• 数据库连接验证：检查应用程序与数据库的连接稳定性，执行多次数据读写操作（如提交申请、修改审批状态），验证数据能正常写入数据库并查询。

• 文件存储验证：测试文件上传功能，上传不同格式、大小的文件，验证文件能正常存储至指定目录，数据库中文件元数据记录完整，文件可正常关联至对应审批记录。

• 安全验证：测试密码修改、登录失败锁定、权限控制等安全功能，验证安全配置生效。

功能验证无问题后，实施团队清理测试数据，备份系统当前配置与数据库数据，向部署单位移交超级管理员账号、核心配置清单、安装日志等资料，填写《系统安装报告》，完成安装收尾工作。

11.3 日常运维规范

日常运维是保障系统长期稳定、安全运行的核心工作，需建立标准化运维流程，明确运维职责与操作规范：

11.3.1 运维职责划分

• 系统管理员：负责系统账号管理（创建、编辑、禁用）、权限调整、参数配置、审批流程优化、日志查询与导出、日常功能问

题排查；

• 数据库管理员：负责数据库性能监控、备份与恢复、索引优化、SQL 语句调优、日志分析、安全配置维护；

• 服务器运维人员：负责服务器硬件监控、操作系统维护、中间件（Nginx/PHP）配置调整、补丁更新、防病毒软件升级、网络连通性保障；

• 安全管理员：负责系统安全监控、漏洞扫描、安全事件处置、合规性检查、日志审计。

11.3.2 日常运维操作流程

• 每日运维检查（1 次/日）：

◦ 系统状态检查：登录管理端，查看系统运行状态（应用服务、数据库服务是否正常），检查核心功能（申请、审批、文件上传）是否可用；

◦ 资源监控：查看服务器 CPU、内存、磁盘空间使用率（磁盘空间剩余不足 20%时触发告警），检查数据库连接数、查询响应时

间；

◦ 日志检查：查看系统错误日志、安全日志，排查异常报错（如数据库连接失败、文件上传失败）、安全事件（如异常登录、越权访问）；

◦ 备份检查：确认前一日数据备份是否成功，备份文件是否完整。

• 每周运维维护（1 次/周）：

◦ 日志清理：清理过期日志（超过留存期限的日志），释放磁盘空间，清理前需备份重要日志；

◦ 数据库优化：分析数据库慢查询日志，优化低效 SQL 语句，检查索引使用情况，必要时重建索引；

◦ 安全扫描：使用自动化工具进行系统安全扫描，排查弱口令、端口开放、漏洞等问题；

◦ 补丁检查：检查操作系统、中间件、数据库的安全补丁，评估是否需要安装（避免盲目打补丁导致兼容性问题）。

• 每月运维总结（1 次/月）：

◦ 性能分析：统计系统月均申请量、并发用户数、响应时间等性能指标，分析性能瓶颈；

◦ 安全评估：汇总月度安全事件、漏洞整改情况，评估系统安全状态；

◦ 运维报告：编制《月度运维报告》，记录运维操作、问题处理、性能数据、安全状况，提出优化建议，上报部署单位负责人。

11.3.3 运维操作规范

• 操作授权：所有运维操作需经授权后方可执行，重要操作（如系统参数修改、数据库结构调整、数据删除）需提交运维申请，经相关负责人审批通过后执行；

• 操作记录：建立运维操作台账，记录操作人、操作时间、操作内容、操作原因、执行结果，确保运维操作可追溯；

• 变更管理：系统配置、代码、数据库结构等变更需遵循变更管理流程，变更前备份相关数据与配置，变更后进行功能验证，确保无衍生问题；

• 权限管控：运维人员账号需遵循最小权限原则，禁止使用超级管理员账号进行日常运维操作；定期清理冗余运维账号，禁用离职人员账号；

• 应急准备：运维人员需熟悉系统应急处理流程，定期演练数据恢复、故障排查等应急操作，确保突发情况能快速响应。

11.4 故障排查与恢复

系统运行过程中可能出现各类故障，需建立标准化故障排查流程与恢复方案，确保故障快速解决，减少业务影响：

11.4.1 常见故障类型与排查流程

• 系统无法访问故障：

◦ 排查步骤：首先检查客户端网络是否正常（测试能否访问其他网站）；其次检查服务器是否正常运行（远程登录服务器，查看

服务器状态）；然后检查 Web 服务（Nginx/Apache）是否启动（执行服务状态查询命令），若未启动则重启服务；最后检查防火墙规则是否拦截访问、端口是否被占用，必要时调整防火墙规则或释放端口。

◦ 恢复措施：若 Web 服务故障，重启服务；若服务器宕机，启动服务器并重启相关服务；若网络故障，联系网络运维人员修复。

• 数据库连接异常故障：

◦ 排查步骤：检查数据库服务是否正常运行（执行数据库状态查询命令），若未运行则重启；检查应用程序数据库配置信息（地址、端口、账号、密码）是否正确；测试数据库服务器网络连通性（ping 数据库服务器、测试 3306 端口）；查看数据库连接数是否达到上限，若达到则调整数据库最大连接数参数；查看数据库日志，排查数据库故障（如磁盘空间不足、权限错误）。

◦ 恢复措施：重启数据库服务；修正应用程序数据库配置；优化数据库连接数参数；清理数据库服务器磁盘空间。

• 文件上传/下载故障（V1.0 仅涉及上传）：

◦ 排查步骤：检查文件上传大小、格式是否超出系统配置限制；查看文件存储目录是否存在、权限是否正确（服务账号是否有读写权限）；检查磁盘空间是否充足；查看系统日志，排查文件上传过程中的报错（如文件读写错误、数据库记录失败）。

◦ 恢复措施：调整文件上传配置参数；修复文件存储目录权限；清理磁盘空间；修复文件上传逻辑错误（若为程序问题）。

• 审批流程异常故障（如审批无法提交、状态不更新）：

◦ 排查步骤：检查审批流程配置是否正确（审批节点、审批人范围是否合理）；查看当前审批人的权限是否有效（账号是否启用、是否具备审批权限）；检查数据库中审批记录数据是否完整（如审批人 ID、审批时间是否为空）；查看系统日志，排查业务逻辑报错。

◦ 恢复措施：修正审批流程配置；调整审批人权限；修复数据库中异常审批记录；修复业务逻辑错误（若为程序问题）。

• 性能卡顿故障：

◦ 排查步骤：查看服务器 CPU、内存、磁盘 I/O 使用率，判断是

否存在资源瓶颈；分析数据库慢查询日志，找出低效 SQL 语句；检查是否存在大量并发请求导致系统过载；查看是否有异常进程占用系统资源。

◦ 恢复措施：优化服务器资源配置（增加 CPU/内存）；优化 SQL 语句与数据库索引；调整系统并发处理参数；终止异常进程。

11.4.2 数据备份与恢复方案

• 数据备份策略：

◦ 数据库备份：采用“实时增量备份+定期全量备份”结合的方式，每日凌晨执行增量备份，每周日凌晨执行全量备份；备份数据存储在独立的备份服务器，采用加密存储，备份文件命名格式为“备份类型_日期_时间.bak”（如 full_20240520_0200.bak）；

◦ 文件备份：用户上传的文件实时同步至备份服务器，采用同步备份工具（如 rsync），确保生产环境文件与备份文件一致；

◦ 备份验证：每周对备份数据进行一次可用性验证，通过恢复测试确认备份文件可正常恢复，记录验证结果。

• 数据恢复流程：

◦ 恢复准备：确认数据丢失或损坏的范围（如某时间段的审批记录、某类文件），明确恢复目标；备份当前系统数据（避免恢复过程中覆盖正常数据）；选择对应的备份文件（全量备份+增量备份）。

◦ 数据库恢复：停止应用服务，避免恢复过程中数据写入；执行数据库恢复命令，先恢复全量备份，再依次恢复后续的增量备份；恢复完成后，启动应用服务，验证数据完整性（查询恢复的数据是否完整、无错乱）。

◦ 文件恢复：停止文件上传服务，从备份服务器复制对应的文件至生产环境文件存储目录；恢复完成后，启动文件上传服务，验证文件可正常访问、关联至对应审批记录。

◦ 恢复总结：记录数据恢复过程、恢复结果、故障原因，编制《数据恢复报告》，上报部署单位负责人，优化备份策略与故障防范措施。

11.4.3 应急响应机制

• 故障分级：

◦ 一级故障（紧急）：系统完全无法使用、数据严重丢失或泄露、大规模安全事件（如黑客攻击），影响核心业务运行；

◦ 二级故障（重要）：核心功能异常（如申请无法提交、审批无法处理），影响部分用户正常使用；

◦ 三级故障（一般）：非核心功能异常（如日志导出格式错误、界面显示错位），不影响核心业务流程。

• 响应流程：

◦ 一级故障：运维人员接到故障报告后，10 分钟内响应，立即启动应急小组，采取紧急措施（如系统隔离、数据备份），4 小时内解决或提供临时替代方案；

◦ 二级故障：30 分钟内响应，2 小时内定位问题，8 小时内解决；

◦ 三级故障：1 小时内响应，24 小时内解决。

• 故障上报：一级故障需立即上报部署单位负责人及实施团队；二级故障需在 2 小时内上报；三级故障可在解决后汇总上报。故障解决后，需进行复盘分析，找出故障根源，制定防范措施，避免类似故障再次发生。

十二、数据库设计

数据库是系统数据存储与管理的核心，本章节详细描述数据库的设计原则、数据表结构、表间关联关系、索引设计及数据安全策略，确保数据库设计合理、高效、安全，支撑系统稳定运行。

12.1 数据库设计原则

系统数据库设计遵循“规范性、高性能、安全性、可扩展性、可追溯”五大核心原则，兼顾数据存储效率、访问速度与长期运维便捷性，为系统稳定运行提供坚实的数据支撑：

• 规范性原则：严格遵循数据库三大范式，确保数据原子性（字段不可拆分）、无部分依赖（非主键字段完全依赖主键）、无传递依赖（非主键字段不依赖其他非主键字段），减少数据冗余，避免同一数据在多表重复存储导致的数据不一致风险；同时合理设

计表结构，平衡范式与查询效率，必要时通过适度冗余（如文件表存储审批编号冗余字段）提升查询性能。

• 高性能原则：针对高频查询场景（如审批记录检索、日志查询）优化表结构与索引设计，建立合理的主键、外键及联合索引，减少查询时的全表扫描；采用分表分库思想（V1.0 采用时间分区表），对日志表等大流量数据表按时间分区存储，提升数据写入与查询效率；优化字段类型选择，优先使用占用空间小、查询效率高的字段类型（如用 INT 存储用户 ID、用 VARCHAR 固定长度存储审批编号），避免不必要的大字段类型。

• 安全性原则：核心敏感数据（如密码哈希、手机号）采用字段级加密存储，加密密钥与数据库分离保管；严格控制数据库账号权限，不同服务账号仅授予最小必要权限（如应用服务账号无 ALTER、DROP 权限）；所有数据表均设置字段非空约束、格式校验约束，确保数据录入合规；通过外键约束维护表间数据一致性，防止非法数据插入。

• 可扩展性原则：数据表结构设计预留扩展字段（如用户表预留“扩展字段 1-3”），支持未来业务需求变更时无需大幅调整表结构；采用模块化表设计，核心业务表（用户表、审批表）与辅助表（字典表、配置表）分离，便于功能扩展与模块升级；字段命

名与表命名遵循统一规范，确保后续维护与二次开发便捷。

• 可追溯原则：核心业务表（审批表、文件表、日志表）均设计创建时间、修改时间、操作人 ID 等审计字段，记录数据全生命周期的操作轨迹；日志表全面覆盖系统关键操作，确保每一次数据变更、功能调用均可追溯，满足审计与合规要求。

12.2 数据库整体架构

系统采用关系型数据库（MySQL 5.7/MariaDB 10.5 及以上）作为核心数据存储引擎，数据库整体架构分为业务数据层、配置数据层、审计数据层三大模块，各模块数据表职责清晰、关联有序：

• 业务数据层：存储核心业务流转数据，是系统运行的核心数据支撑，包括用户表、部门表、角色表、审批表、文件表等，记录用户信息、用章申请、审批流转、文件存储等关键业务数据，表间通过主键-外键关联形成完整业务数据链。

• 配置数据层：存储系统运行所需的配置参数与基础字典数据，包括系统配置表、审批流程配置表、数据字典表等，支撑系统参数动态调整、审批流程灵活配置，无需修改代码即可适配不同部

署单位的业务需求。

• 审计数据层：存储系统所有操作审计日志，包括登录日志表、操作日志表、安全日志表等，全面记录用户登录、业务操作、系统运行、安全事件等信息，为审计追溯、安全排查提供依据。

数据库采用 UTF-8 编码格式，确保支持中文、特殊字符的正常存储与显示；数据库存储引擎优先使用 InnoDB，支持事务、行级锁与外键约束，保障高并发场景下的数据一致性与访问性能。

12.3 核心数据表结构设计

12.3.1 用户表（sys_user）

用户表存储系统所有用户的基础信息与账号状态，是账号体系与权限管理的核心表，结构设计如下：

• 用户 ID（user_id）：INT 类型，主键，自增，唯一标识，无空值约束，用于关联其他数据表；

• 用户名（username）：VARCHAR(20)类型，唯一索引，无空值约束，支持字母、数字组合，作为用户登录唯一凭证；

• 昵称（nickname）：VARCHAR(30)类型，无空值约束，存储用户显示名称；

• 密码哈希（password_hash）：VARCHAR(64)类型，无空值约束，采用 SHA-256 不可逆哈希算法加密存储，不存储明文密码；

• 所属部门 ID（dept_id）：INT 类型，外键，关联部门表（sys_dept）的部门 ID，无空值约束，标识用户所属部门；

• 角色 ID（role_id）：INT 类型，外键，关联角色表（sys_role）的角色 ID，无空值约束，标识用户所属角色；

• 手机号（phone）：VARCHAR(16)类型，唯一约束，字段级加密存储，用于紧急联系与身份核验；

• 账号状态（status）：TINYINT 类型，无空值约束，0-禁用、1-启用，控制账号登录权限；

• 最后登录时间（last_login_time）：DATETIME 类型，可空，记录用户最近一次登录时间；

• 最后登录 IP（last_login_ip）：VARCHAR(32)类型，可空，记录用户最近一次登录 IP 地址；

• 创建人 ID（create_by）：INT 类型，无空值约束，关联用户表自身的用户 ID，记录账号创建人；

• 创建时间（create_time）：DATETIME 类型，无空值约束，默认当前时间，记录账号创建时间；

• 修改人 ID（update_by）：INT 类型，可空，关联用户表自身的用户 ID，记录账号最后修改人；

• 修改时间（update_time）：DATETIME 类型，可空，记录账号最后修改时间；

• 扩展字段 1-3（ext1-ext3）：VARCHAR(50)类型，可空，预留用于未来业务扩展。

12.3.2 部门表（sys_dept）

部门表存储部署单位的组织架构信息，支持多级部门嵌套，结构设计如下：

• 部门 ID（dept_id）：INT 类型，主键，自增，唯一标识，无空值约束；

• 部门名称（dept_name）：VARCHAR(50)类型，无空值约束，唯一约束（同一层级部门名称不可重复），存储部门全称；

• 部门代号（dept_code）：VARCHAR(20)类型，无空值约束，唯一约束，用于审批编号生成、数据分类等场景；

• 上级部门 ID（parent_id）：INT 类型，外键，关联部门表自身的部门 ID，顶级部门父 ID 为 0，支持多级部门架构；

• 部门负责人 ID（leader_id）：INT 类型，外键，关联用户表（sys_user）的用户 ID，可空，标识部门负责人；

• 部门排序（sort）：INT 类型，无空值约束，默认 0，用于部门列表显示排序；

• 部门状态（status）：TINYINT 类型，无空值约束，0-禁用、1-启用，控制部门是否可用；

• 创建人 ID（create_by）：INT 类型，无空值约束，关联用户表的用户 ID；

• 创建时间（create_time）：DATETIME 类型，无空值约束，默认当前时间；

• 修改人 ID（update_by）：INT 类型，可空，关联用户表的用户 ID；

• 修改时间（update_time）：DATETIME 类型，可空。

12.3.3 角色表（sys_role）

角色表存储系统角色定义与权限关联信息，是 RBAC 权限模型的核心表，结构设计如下：

• 角色 ID（role_id）：INT 类型，主键，自增，唯一标识，无空值约束；

• 角色名称（role_name）：VARCHAR(30)类型，无空值约束，唯一约束，如“普通用户”“审批员”“系统管理员”；

• 角色描述（role_desc）：VARCHAR(200)类型，可空，描述角色的权限范围与适用场景；

• 角色状态（status）：TINYINT 类型，无空值约束，0-禁用、1-启用；

• 创建人 ID（create_by）：INT 类型，无空值约束，关联用户表的用户 ID；

• 创建时间（create_time）：DATETIME 类型，无空值约束，默认当前时间；

• 修改人 ID（update_by）：INT 类型，可空，关联用户表的用户 ID；

• 修改时间（update_time）：DATETIME 类型，可空。

12.3.4 权限表（sys_permission）

权限表存储系统所有操作权限的基础信息，是权限控制的最小单位，结构设计如下：

• 权限 ID（perm_id）：INT 类型，主键，自增，唯一标识，无空值约束；

• 权限名称（perm_name）：VARCHAR(50)类型，无空值约束，唯一约束，如“提交用章申请”“审批用章申请”“导出日志”；

• 权限标识（perm_key）：VARCHAR(100)类型，无空值约束，唯一约束，用于代码中权限校验，如“seal:apply:submit”“seal:approve:pass”；

• 权限类型（perm_type）：TINYINT 类型，无空值约束，0-菜单权限、1-按钮权限、2-接口权限，标识权限适用场景；

• 上级权限 ID（parent_id）：INT 类型，外键，关联权限表自身的权限 ID，支持权限层级划分；

• 排序（sort）：INT 类型，无空值约束，默认 0，用于权限列表显示排序；

• 创建时间（create_time）：DATETIME 类型，无空值约束，默认当前时间；

• 修改时间（update_time）：DATETIME 类型，可空。

12.3.5 角色权限关联表（sys_role_perm）

角色权限关联表是角色与权限的中间关联表，实现多对多关联（一个角色可关联多个权限，一个权限可关联多个角色），结构设计如下：

• 关联 ID（id）：INT 类型，主键，自增，唯一标识，无空值约束；

• 角色 ID（role_id）：INT 类型，外键，关联角色表（sys_role）的角色 ID，无空值约束；

• 权限 ID（perm_id）：INT 类型，外键，关联权限表（sys_permission）的权限 ID，无空值约束；

• 唯一约束：角色 ID+权限 ID 组合唯一，避免重复授权；

• 创建时间（create_time）：DATETIME 类型，无空值约束，默认当前时间。

12.3.6 审批表（seal_approval）

审批表是系统核心业务表，存储用章申请的全流程信息，记录申请、审批、盖章、归档等全生命周期数据，结构设计如下：

• 审批 ID（approval_id）：BIGINT 类型，主键，自增，唯一标识，无空值约束，用于关联文件表、审批记录表；

• 审批编号（approval_no）：VARCHAR(30)类型，唯一索引，无空值约束，系统自动生成，格式可配置（如“2024-DEP01-00001”），是用章申请的唯一业务标识；

• 申请人 ID（apply_user_id）：INT 类型，外键，关联用户表（sys_user）的用户 ID，无空值约束，标识申请发起者；

• 所属部门 ID（dept_id）：INT 类型，外键，关联部门表（sys_dept）的部门 ID，无空值约束，标识申请所属部门；

• 申请标题（title）：VARCHAR(50)类型，无空值约束，简要描述用章用途，如“XX 项目合作协议盖章申请”；

• 用章用途（purpose）：TINYINT 类型，无空值约束，关联数据

字典表（sys_dict），如 0-合同签署、1-公文用印、2-证明文件、3-其他；

• 文件类型（file_type）：VARCHAR(50)类型，无空值约束，存储申请材料的文件类型组合，如“Word,PDF,图片”；

• 申请说明（remark）：TEXT 类型，无空值约束，详细描述用章背景、文件数量、紧急程度等信息；

• 紧急程度（urgent_level）：TINYINT 类型，无空值约束，0-普通、1-紧急、2-特急，默认 0；

• 预计用章时间（plan_seal_time）：DATE 类型，可空，记录申请人预计的用章时间；

• 申请状态（status）：TINYINT 类型，无空值约束，0-待审批、1-审批中、2-已通过、3-已驳回、4-待盖章、5-已归档、6-已撤回，标识申请当前状态；

• 审批人 ID（approve_user_id）：INT 类型，外键，关联用户表（sys_user）的用户 ID，可空，标识最终审批人；

• 审批时间（approve_time）：DATETIME 类型，可空，记录审批通过/驳回的时间；

• 驳回意见（reject_reason）：TEXT 类型，可空，仅当状态为“已驳回”时填写；

• 盖章人 ID（seal_user_id）：INT 类型，外键，关联用户表（sys_user）的用户 ID，可空，标识执行盖章操作的人员；

• 盖章时间（seal_time）：DATETIME 类型，可空，记录盖章文件上传并归档的时间；

• 提交设备信息（submit_device）：VARCHAR(100)类型，可空，记录申请提交时的设备型号、操作系统等信息；

• 提交 IP 地址（submit_ip）：VARCHAR(32)类型，可空，记录申请提交时的 IP 地址；

• 创建时间（create_time）：DATETIME 类型，无空值约束，默认当前时间，记录申请提交时间；

• 修改时间（update_time）：DATETIME 类型，可空，记录申请

状态或信息最后修改时间；

• 扩展字段 1-2（ext1-ext2）：VARCHAR(100)类型，可空，预留用于业务扩展（如项目编号、合同金额等自定义字段）。

12.3.7 审批记录明细表（seal_approval_record）

审批记录明细表存储审批流程各节点的处理记录，形成完整审批链，结构设计如下：

• 记录 ID（record_id）：BIGINT 类型，主键，自增，唯一标识，无空值约束；

• 审批 ID（approval_id）：BIGINT 类型，外键，关联审批表（seal_approval）的审批 ID，无空值约束；

• 审批节点 ID（node_id）：INT 类型，外键，关联审批流程配置表（seal_approval_flow）的节点 ID，无空值约束，标识当前审批节点；

• 处理人 ID（deal_user_id）：INT 类型，外键，关联用户表（sys_user）的用户 ID，无空值约束，标识该节点处理人；

• 处理类型（deal_type）：TINYINT 类型，无空值约束，0-通过、1-驳回、2-转签，标识处理结果；

• 处理意见（deal_remark）：TEXT 类型，可空，记录处理人的具体意见；

• 处理时间（deal_time）：DATETIME 类型，无空值约束，默认当前时间，记录节点处理时间；

• 处理 IP 地址（deal_ip）：VARCHAR(32)类型，可空，记录处理时的 IP 地址；

• 处理设备信息（deal_device）：VARCHAR(100)类型，可空，记录处理时的设备信息。

12.3.8 文件表（seal_file）

文件表存储用户上传的申请材料、盖章文件等电子文件的元数据信息，是文件存储与关联的核心表，确保文件可追溯、可校验，结构设计如下：

• 文件 ID（file_id）：BIGINT 类型，主键，自增，唯一标识，无空值约束，作为文件的全局唯一索引；

• 审批 ID（approval_id）：BIGINT 类型，外键，关联审批表（seal_approval）的审批 ID，无空值约束，确保文件与用章申请一一对应，形成业务关联；

• 文件名称（file_name）：VARCHAR(255)类型，无空值约束，存储文件原始名称（含后缀），保留用户上传时的文件标识，如“XX 项目合作协议_v1.docx”；

• 文件存储路径（file_path）：VARCHAR(512)类型，无空值约束，存储文件在服务器本地受控目录的绝对路径，采用“日期目录+加密文件名”的命名规则（如“/data/seal-files/20240520/7f9d21c8-3e4b-4a12-b567-890a3d2f1e7c.pdf”），避免路径泄露与文件覆盖；

• 文件类型（file_type）：VARCHAR(50)类型，无空值约束，存储文件的 MIME 类型，如“application/vnd.openxmlformats-officedocument.wordprocessingml.document”（Word 文档）、“application/pdf”（PDF 文件）、“image/jpeg”（JPG 图片），用于文件格式校验与识别；

• 文件大小（file_size）：BIGINT 类型，无空值约束，以字节（Byte）为单位记录文件实际大小，便于存储容量统计与上传大小限制校验；

• 文件哈希值（file_hash）：VARCHAR(64)类型，无空值约束，采用 MD5 算法计算文件的唯一校验码，每一份文件对应唯一哈希值，用于验证文件传输与存储过程中的完整性，防止文件被篡改；

• 文件来源（file_source）：TINYINT 类型，无空值约束，0-申请材料（用户端上传的用章申请附件）、1-盖章文件（盖章端上传的已盖章文件），明确文件用途分类；

• 上传人 ID（upload_user_id）：INT 类型，外键，关联用户表（sys_user）的用户 ID，无空值约束，记录文件上传人的身份信息，便于追溯责任；

• 上传时间（upload_time）：DATETIME 类型，无空值约束，默认当前时间（精确到毫秒），记录文件上传的具体时间节点；

• 文件状态（file_status）：TINYINT 类型，无空值约束，0-正

常（文件有效且可关联查询）、1-已替换（文件被同一审批 ID 下的新文件替换）、2-已删除（文件逻辑删除，保留元数据），默认 0，支持文件的柔性管理；

• 替换文件 ID（replace_file_id）：BIGINT 类型，可空，外键关联文件表自身的文件 ID，仅当文件状态为“已替换”时填写，记录被替换的原文件 ID，形成文件变更轨迹；

• 备注（remark）：VARCHAR(200)类型，可空，存储文件相关的补充说明，如“合同正文附件”“盖章页扫描件”；

• 创建时间（create_time）：DATETIME 类型，无空值约束，默认当前时间，与上传时间保持一致，作为数据审计的基础字段；

• 修改时间（update_time）：DATETIME 类型，可空，记录文件状态变更（如替换、删除）的时间，关联修改人 ID；

• 修改人 ID（update_by）：INT 类型，可空，外键关联用户表（sys_user）的用户 ID，记录修改文件状态的操作人员。

12.3.9 审批流程配置表（seal_approval_flow）

审批流程配置表存储用章申请的审批节点与流转规则，支持不同用章类型的差异化流程配置，结构设计如下：

• 流程 ID（flow_id）：INT 类型，主键，自增，唯一标识，无空值约束；

• 流程名称（flow_name）：VARCHAR(50)类型，无空值约束，唯一约束，如“合同签署审批流程”“公文用印审批流程”，明确流程适用场景；

• 用章用途类型（purpose_type）：TINYINT 类型，无空值约束，关联数据字典表（sys_dict）的用章用途编码，如 0-合同签署、1-公文用印，实现“用章用途-审批流程”的绑定；

• 流程状态（status）：TINYINT 类型，无空值约束，0-禁用、1-启用，控制流程是否可被使用；

• 驳回规则（reject_rule）：TINYINT 类型，无空值约束，0-驳回至申请人（修改后重新提交全流程）、1-驳回至上一节点（仅需上一节点重新审批），定义驳回后的流转逻辑；

• 紧急审批时效（urgent_timeout）：INT 类型，可空，单位为

小时，仅针对紧急程度为“紧急/特急”的申请，设置审批节点的最长处理时限，超时触发提醒；

• 备注（remark）：VARCHAR(200)类型，可空，记录流程配置的补充说明，如“需法务部门审核的合同专用流程”；

• 创建人 ID（create_by）：INT 类型，无空值约束，关联用户表（sys_user）的用户 ID；

• 创建时间（create_time）：DATETIME 类型，无空值约束，默认当前时间；

• 修改人 ID（update_by）：INT 类型，可空，关联用户表（sys_user）的用户 ID；

• 修改时间（update_time）：DATETIME 类型，可空。

12.3.10 审批流程节点表（seal_approval_node）

审批流程节点表存储单个审批流程的具体节点配置，定义每个节点的审批人、权限与流转规则，结构设计如下：

• 节点 ID（node_id）：INT 类型，主键，自增，唯一标识，无空值约束；

• 流程 ID（flow_id）：INT 类型，外键，关联审批流程配置表（seal_approval_flow）的流程 ID，无空值约束，标识节点所属流程；

• 节点名称（node_name）：VARCHAR(30)类型，无空值约束，如“部门负责人审批”“法务审核”“分管领导签批”；

• 节点排序（node_sort）：INT 类型，无空值约束，如 1、2、3，定义审批节点的流转顺序；

• 审批人类型（approver_type）：TINYINT 类型，无空值约束，0-指定用户（直接关联具体用户 ID）、1-部门负责人（关联申请所属部门的负责人）、2-角色组（关联特定角色的所有用户），灵活配置审批人来源；

• 关联 ID（related_id）：INT 类型，无空值约束，根据审批人类型关联对应数据：审批人类型为 0 时关联用户表（sys_user）的用户 ID，类型为 1 时关联部门表（sys_dept）的部门 ID，类型为 2 时关联角色表（sys_role）的角色 ID；

• 节点权限（node_perm）：TINYINT 类型，无空值约束，0-仅审批（通过/驳回）、1-审批+修改申请信息、2-审批+补充意见，定义节点审批人的操作权限；

• 多人审批规则（multi_rule）：TINYINT 类型，无空值约束，0-单人审批（任意关联用户通过即可）、1-多人会签（所有关联用户通过方可），适用于多角色共同审批场景；

• 超时提醒方式（timeout_remind）：TINYINT 类型，可空，0-系统消息提醒、1-短信提醒（需后续启用短信模块），默认 0，设置超时后的提醒方式；

• 创建时间（create_time）：DATETIME 类型，无空值约束，默认当前时间；

• 修改时间（update_time）：DATETIME 类型，可空。

12.3.11 登录日志表（sys_login_log）

登录日志表记录所有用户的登录行为，为账号安全审计提供依据，结构设计如下：

• 日志 ID（log_id）：BIGINT 类型，主键，自增，唯一标识，无空值约束；

• 用户名（username）：VARCHAR(20)类型，无空值约束，关联用户表（sys_user）的用户名，记录登录账号；

• 用户 ID（user_id）：INT 类型，可空，关联用户表（sys_user）的用户 ID，账号存在时自动关联；

• 登录 IP 地址（login_ip）：VARCHAR(32)类型，无空值约束，记录登录时的客户端 IP 地址（支持 IPv4/IPv6 格式）；

• 登录设备（login_device）：VARCHAR(100)类型，可空，记录登录设备型号、操作系统版本，如“iPhone 14 iOS 16.5”“Windows 11 Chrome 120.0”；

• 登录地点（login_location）：VARCHAR(50)类型，可空，根据 IP 地址解析的省/市/区信息，如“北京市朝阳区”；

• 登录结果（login_result）：TINYINT 类型，无空值约束，0-失败、1-成功，标识登录状态；

• 失败原因（fail_reason）：VARCHAR(100)类型，可空，仅登录失败时填写，如“密码错误”“账号禁用”“登录次数超限锁定”；

• 登录时间（login_time）：DATETIME 类型，无空值约束，默认当前时间（精确到毫秒）；

• 会话 ID（session_id）：VARCHAR(64)类型，可空，记录登录成功后生成的会话标识，用于关联会话生命周期；

• 退出时间（logout_time）：DATETIME 类型，可空，记录用户主动退出或会话超时的时间。

12.3.12 操作日志表（sys_operate_log）

操作日志表记录用户在系统内的所有业务操作行为，形成完整的操作审计链，结构设计如下：

• 日志 ID（log_id）：BIGINT 类型，主键，自增，唯一标识，无空值约束；

• 操作人 ID（operate_user_id）：INT 类型，无空值约束，关联用户表（sys_user）的用户 ID，记录操作人身份；

• 操作人名称（operate_user_name）：VARCHAR(30)类型，无空值约束，存储操作人昵称（冗余字段，便于快速查询）；

• 所属部门 ID（dept_id）：INT 类型，无空值约束，关联部门表（sys_dept）的部门 ID，标识操作人所属部门；

• 操作模块（operate_module）：VARCHAR(30)类型，无空值约束，如“用章申请”“审批管理”“账号管理”“系统配置”，明确操作所属功能模块；

• 操作类型（operate_type）：VARCHAR(20)类型，无空值约束，如“新增”“修改”“删除”“查询”“导出”“提交”“审批”，定义操作行为；

• 操作对象（operate_object）：VARCHAR(50)类型，无空值约束，记录操作的具体对象，如“审批单（编号：2024-DEP01-00001）”“用户账号（admin）”；

• 操作 IP 地址（operate_ip）：VARCHAR(32)类型，无空值约

束，记录操作时的客户端 IP 地址；

• 操作设备（operate_device）：VARCHAR(100)类型，可空，记录操作设备信息；

• 操作结果（operate_result）：TINYINT 类型，无空值约束，0-失败、1-成功，标识操作是否完成；

• 操作内容（operate_content）：TEXT 类型，可空，详细记录操作的具体内容，如“提交用章申请，标题：XX 项目合作协议盖章申请，用章用途：合同签署”“审批通过编号为 2024-DEP01-00001 的申请，审批意见：同意”；

• 错误信息（error_msg）：TEXT 类型，可空，仅操作失败时填写，记录错误详情（如“文件大小超出限制”“权限不足”）；

• 操作时间（operate_time）：DATETIME 类型，无空值约束，默认当前时间（精确到毫秒）；

• 备注（remark）：VARCHAR(200)类型，可空，补充记录操作相关的特殊信息。

12.3.13 系统配置表（sys_config）

系统配置表存储系统运行所需的全局参数配置，支持动态调整系统行为，无需修改代码，结构设计如下：

• 配置 ID（config_id）：INT 类型，主键，自增，唯一标识，无空值约束；

• 配置键（config_key）：VARCHAR(50)类型，无空值约束，唯一约束，如“password_strength”“approval_no_rule”“file_upload_max_size”，作为配置参数的唯一标识；

• 配置值（config_value）：TEXT 类型，可空，存储配置参数的具体值，如“12 位（含大小写字母+数字+特殊符号）”“{year}-{dept_code}-{seq:5}”“209715200”（200MB 对应的字节数）；

• 配置名称（config_name）：VARCHAR(100)类型，无空值约束，如“密码复杂度要求”“审批编号生成规则”“单个文件上传最大限制”；

• 配置类型（config_type）：VARCHAR(30)类型，无空值约束，如“安全配置”“业务配置”“存储配置”“日志配置”，对配置参

数分类；

• 备注（remark）：VARCHAR(200)类型，可空，说明配置参数的用途与生效范围，如“密码复杂度要求仅适用于新注册账号及密码修改”；

• 排序（sort）：INT 类型，无空值约束，默认 0，用于配置列表显示排序；

• 创建时间（create_time）：DATETIME 类型，无空值约束，默认当前时间；

• 修改时间（update_time）：DATETIME 类型，可空；

• 修改人 ID（update_by）：INT 类型，可空，关联用户表（sys_user）的用户 ID。

12.3.14 数据字典表（sys_dict）

数据字典表存储系统通用的枚举类型数据，如用章用途、紧急程度、账号状态等，统一数据标准，结构设计如下：

• 字典 ID（dict_id）：INT 类型，主键，自增，唯一标识，无空值约束；

• 字典类型（dict_type）：VARCHAR(50)类型，无空值约束，如“seal_purpose”（用章用途）、“urgent_level”（紧急程度）、“user_status”（账号状态），标识字典所属类别；

• 字典编码（dict_code）：VARCHAR(30)类型，无空值约束，唯一约束（同一字典类型下编码唯一），如“contract”“urgent”“enabled”，作为字典项的唯一标识；

• 字典值（dict_value）：VARCHAR(100)类型，无空值约束，如“合同签署”“紧急”“启用”，字典项的显示名称；

• 排序（sort）：INT 类型，无空值约束，默认 0，控制字典项的显示顺序；

• 状态（status）：TINYINT 类型，无空值约束，0-禁用、1-启用，控制字典项是否可用；

• 备注（remark）：VARCHAR(200)类型，可空，说明字典项的适用场景；

• 创建时间（create_time）：DATETIME 类型，无空值约束，默认当前时间；

• 修改时间（update_time）：DATETIME 类型，可空。

12.4 表间关联关系

系统数据表通过主键-外键严格关联，形成逻辑清晰、数据一致的关系网络，确保业务数据流转的完整性与准确性，核心关联关系如下：

• 部门与用户：部门表（sys_dept）的部门 ID（dept_id）作为外键，关联用户表（sys_user）的所属部门 ID（dept_id）。关联类型为一对多，即一个部门可包含多个用户（如“市场部”下有多名普通用户），一个用户仅归属一个部门，确保用户组织归属唯一。

• 角色与用户：角色表（sys_role）的角色 ID（role_id）作为外键，关联用户表（sys_user）的角色 ID（role_id）。关联类型为一对多，即一个角色可分配给多个用户（如“审批员”角色分配给多名部门负责人），V1.0 版本支持用户单角色关联，后续

可扩展多角色关联能力，确保用户权限边界清晰。

• 角色与权限：通过角色权限关联表（sys_role_perm）实现多对多关联——角色表（sys_role）的角色 ID（role_id）与权限表（sys_permission）的权限 ID（perm_id）分别作为外键，存入关联表。一个角色可关联多个权限（如“系统管理员”关联账号管理、日志导出等所有权限），一个权限可关联多个角色（如“查询审批记录”权限同时关联审批员、管理员角色），灵活实现权限批量分配。

• 审批流程与节点：审批流程配置表（seal_approval_flow）的流程 ID（flow_id）作为外键，关联审批流程节点表（seal_approval_node）的流程 ID（flow_id）。关联类型为一对多，即一个审批流程可包含多个审批节点（如“合同签署流程”包含部门负责人审批、法务审核、分管领导签批 3 个节点），一个节点仅归属一个流程，确保流程与节点的绑定唯一性。

• 审批与文件：审批表（seal_approval）的审批 ID（approval_id）作为外键，关联文件表（seal_file）的审批 ID（approval_id）。关联类型为一对多，即一个用章申请可关联多个文件（如 1 份申请包含 3 份申请材料+1 份盖章文件），一个文件仅关联一个审批，确保文件与业务申请的精准绑定。

• 审批与审批记录：审批表（seal_approval）的审批 ID（approval_id）作为外键，关联审批记录明细表（seal_approval_record）的审批 ID（approval_id）。关联类型为一对多，即一个审批流程可对应多条节点处理记录（如 3 个审批节点对应 3 条处理记录），完整记录审批链流转轨迹，确保审批过程可追溯。

• 审批流程与用章用途：审批流程配置表（seal_approval_flow）的用章用途类型（purpose_type）作为外键，关联数据字典表（sys_dict）的字典编码（dict_code）。关联类型为一对多，即一个用章用途可绑定一个审批流程（如“合同签署”用途绑定专属审批流程），一个审批流程可适配一个或多个用章用途（需通过字典表关联配置），实现差异化流程管控。

• 操作日志与用户/部门：操作日志表（sys_operate_log）的操作人 ID（operate_user_id）、所属部门 ID（dept_id）分别作为外键，关联用户表（sys_user）的用户 ID（user_id）、部门表（sys_dept）的部门 ID（dept_id）。关联类型为多对一，即多条操作日志可归属同一用户或同一部门，便于按用户、部门维度追溯操作行为。

所有表间关联均启用外键约束，当主表记录删除或修改时，从表关联记录将触发约束行为（如主表部门删除时，禁止删除存在关联用户的部门；主表审批记录删除时，级联删除关联的文件记录），确保数据一致性，避免孤儿数据产生。

12.5 索引设计

为提升数据库查询效率，降低高并发场景下的性能瓶颈，系统针对核心数据表设计了合理的索引体系，遵循“高频查询字段优先、联合索引适配多条件查询、避免过度索引”的原则，核心索引设计如下：

• 主键索引：所有数据表均以主键字段（如 user_id、approval_id、file_id）创建主键索引（PRIMARY KEY），主键字段采用自增 INT/BIGINT 类型，确保数据插入时索引有序增长，提升写入性能，同时保障主键查询（如通过审批 ID 查询申请详情）的响应速度。

• 唯一索引：针对需唯一约束的业务字段创建唯一索引（UNIQUE KEY），包括：

◦ 用户表（sys_user）：用户名（username）、手机号（phone），避免重复账号或手机号；

◦ 审批表（seal_approval）：审批编号（approval_no），确保审批编号全局唯一；

◦ 部门表（sys_dept）：部门名称（dept_name）、部门代号（dept_code），避免同一层级部门名称或代号重复；

◦ 角色表（sys_role）：角色名称（role_name），确保角色名称唯一；

◦ 权限表（sys_permission）：权限标识（perm_key），确保权限标识唯一。

• 普通索引：针对高频查询、排序、关联字段创建普通索引（INDEX），包括：

◦ 用户表（sys_user）：所属部门 ID（dept_id）、角色 ID（role_id），适配按部门、角色查询用户列表的场景；

◦ 审批表（seal_approval）：申请人 ID（apply_user_id）、所

属部门 ID（dept_id）、申请状态（status）、用章用途（purpose）、创建时间（create_time），适配按申请人、部门、状态、用途、时间查询审批记录的场景；

◦ 文件表（seal_file）：审批 ID（approval_id）、上传人 ID（upload_user_id）、文件来源（file_source），适配按审批 ID 关联文件、按上传人查询文件的场景；

◦ 审批记录明细表（seal_approval_record）：审批 ID（approval_id）、处理人 ID（deal_user_id），适配查询审批节点处理记录的场景；

◦ 操作日志表（sys_operate_log）：操作人 ID（operate_user_id）、所属部门 ID（dept_id）、操作模块（operate_module）、操作时间（operate_time），适配按用户、部门、模块、时间查询操作日志的场景；

◦ 登录日志表（sys_login_log）：用户名（username）、登录时间（login_time）、登录 IP 地址（login_ip），适配查询用户登录轨迹的场景。

• 联合索引：针对多条件组合查询场景创建联合索引，提升复杂

查询效率，包括：

◦ 审批表（seal_approval）：所属部门 ID（dept_id）+ 申请状态（status）+ 创建时间（create_time），适配“查询某部门近 30 天待审批申请”等高频组合查询；

◦ 操作日志表（sys_operate_log）：操作模块（operate_module）+ 操作时间（operate_time）+ 操作结果（operate_result），适配“查询某模块当天成功的操作记录”等场景；

◦ 审批记录明细表（seal_approval_record）：审批 ID（approval_id）+ 节点排序（node_sort），适配按审批 ID 查询节点流转顺序的场景。

索引维护方面，系统定期（建议每周）分析索引使用情况，删除冗余索引、优化低效索引；针对日志表等大流量表，结合时间分区表特性，确保索引仅作用于当前分区，提升查询效率。

12.6 数据安全与存储策略

12.6.1 数据安全设计

• 敏感数据加密：用户密码采用 SHA-256 不可逆哈希算法加密存储，加密时加入随机盐值（Salt），防止彩虹表破解；手机号等敏感字段采用 AES-256 字段级加密存储，加密密钥由部署单位专人保管，与数据库分离存储，仅授权接口可解密访问。

• 数据访问控制：数据库账号按最小权限原则分配，应用服务账号仅具备 SELECT、INSERT、UPDATE、DELETE 权限，无 ALTER、DROP、CREATE 权限；数据库远程访问仅允许应用服务器 IP，禁用公网直接访问；敏感数据查询需通过系统接口，接口层增加权限校验，确保仅授权用户可访问。

• 数据完整性保障：通过字段非空约束、数据类型约束、外键约束确保数据录入合规；文件表的文件哈希值（MD5）与文件内容绑定，定期校验文件完整性，防止文件被篡改；核心业务数据（如审批记录、日志）的修改操作需记录变更日志，保留原始数据。

• 数据备份与恢复：采用“实时增量备份+定期全量备份”策略，数据库每日凌晨执行增量备份，每周日凌晨执行全量备份，备份数据存储在独立的加密备份服务器，备份文件保留周期不少于 1 年；支持按时间点恢复数据，恢复前需进行数据一致性校

验，确保恢复后数据无错乱。

12.6.2 数据存储策略

• 存储介质选择：数据库数据、系统文件优先存储在企业级 SSD 硬盘，提升读写速度；备份数据存储在 SAS 硬盘或磁带库，兼顾存储成本与数据安全性。

• 分区表设计：针对日志表（sys_login_log、sys_operate_log）等大流量数据表，采用按时间分区存储（按月份分区），每个分区独立存储、管理，提升数据写入与查询效率；分区满一定周期（如 1 年）后，可将历史分区数据归档至低成本存储介质，释放主存储空间。

• 数据生命周期管理：核心业务数据（审批表、文件表、用户表）长期存储，直至满足法定留存期限后按规定销毁；日志数据默认留存 1 年，超过留存期限后自动归档或清理；临时数据（如会话数据）在会话过期后自动删除，释放存储资源。

• 存储容量规划：根据部署单位用户规模、日均申请量、文件大小预估存储容量，预留不少于 50%的冗余空间；定期监控存储容量使用情况，当剩余空间不足 20%时触发告警，及时扩容或清理

过期数据。

12.7 数据库优化策略

为确保数据库在高并发、大数据量场景下稳定运行，系统从查询、写入、索引、配置四个维度制定优化策略：

• 查询优化：规范 SQL 语句编写，避免 SELECT * 、子查询嵌套过深、模糊查询（%前缀）等低效写法；高频查询结果通过 Redis 缓存（可选）缓存，减少数据库访问压力；分页查询采用“基于主键 ID 分页”替代“LIMIT 大偏移量”，提升大数据量分页效率；定期分析慢查询日志（阈值设为 1 秒），优化低效 SQL 语句与索引。

• 写入优化：批量插入数据（如批量导入历史审批记录）采用 INSERT INTO ... VALUES (...) 批量语法，减少数据库连接开销；核心业务写入（如审批提交、文件上传）采用事务机制，确保数据一致性，同时控制事务粒度，避免长事务占用数据库资源；非核心数据写入（如日志记录）采用异步写入方式，提升用户操作响应速度。

• 索引优化：定期（每周）通过 EXPLAIN 分析索引使用情况，删

除未使用、冗余索引；针对频繁更新的字段（如审批状态），评估索引必要性，避免索引频繁失效；大表添加索引时采用在线 DDL 方式，避免锁表影响业务运行。

• 配置优化：调整数据库核心配置参数，提升性能上限，包括：

◦ 连接池配置：max_connections（最大连接数）设为 1000-2000，wait_timeout（连接超时时间）设为 300 秒，避免连接耗尽；

◦ 缓存配置：innodb_buffer_pool_size（InnoDB 缓冲池大小）设为服务器内存的 50%-70%，提升数据缓存命中率；query_cache_type（查询缓存类型）设为 OFF，避免查询缓存失效导致的性能损耗；

◦ 日志配置：slow_query_log（慢查询日志）设为 ON，long_query_time（慢查询阈值）设为 1 秒，便于定位低效查询；

◦ 写入优化：innodb_flush_log_at_trx_commit 设为 1（确保事务 ACID 特性），innodb_log_buffer_size 设为 64M，提升写入性能；

◦ 分区配置：开启 innodb_file_per_table，确保每个表独立表空间，便于分区管理与数据清理。

十三、API 接口说明

系统 API 接口采用 RESTful 设计风格，遵循“资源导向、HTTP 方法语义化、接口标准化”原则，为前端页面、第三方系统集成提供统一、高效、安全的接口服务。本章节详细说明接口命名规范、认证方式、请求/响应格式及核心接口功能，所有接口均已完成标准化实现与文档化说明。

13.1 接口设计规范

13.1.1 命名规范

• 资源命名：采用名词复数形式，描述接口操作的资源对象，如“/api/users”（用户资源）、“/api/approvals”（审批资源）、“/api/files”（文件资源），避免使用动词。

• 接口路径：采用“/api/[资源名称]/[子资源名称]”的层级结构，如“/api/approvals/{approvalId}/records”（审批记录子

资源)、“/api/users/{userId}/login-logs”(用户登录日志子资源)。

• HTTP 方法语义：严格遵循 HTTP 方法的语义化使用，GET（查询资源)、POST（创建资源)、PUT（全量更新资源)、PATCH（部分更新资源)、DELETE（删除资源)，避免跨语义使用。

• 版本控制：接口路径中包含版本号，如“/api/v1/users”，便于后续接口迭代升级，保障兼容性。

• 参数命名：请求参数（路径参数、查询参数、请求体参数）采用小驼峰命名法（如“applyUserId”“deptId”)，与数据库字段命名（下划线命名）通过代码自动映射，确保前后端命名规范统一。

13.1.2 认证与授权规范

• 认证方式：采用基于 Token 的身份认证机制，用户登录成功后，服务器生成唯一的 JWT（JSON Web Token）令牌，返回给客户端；客户端后续所有请求需在 HTTP 请求头中携带“Authorization: Bearer {token}”，服务器验证 Token 有效性(有效期、签名）后，才允许访问接口。

• Token 有效期：Token 默认有效期为 2 小时（可通过系统配置调整），有效期届满后，客户端需重新登录获取新 Token；支持 Token 刷新机制，客户端可通过刷新接口（/api/v1/auth/refresh-token）获取新 Token，避免频繁登录。

• 授权校验：接口层集成权限校验拦截器，根据 Token 解析的用户角色与权限，校验用户是否具备访问当前接口的权限；未授权用户访问需权限的接口时，返回 403 Forbidden 错误。

13.1.3 请求与响应规范

• 请求格式：支持 HTTP/HTTPS 协议，请求体数据格式为 JSON（Content-Type: application/json）；文件上传接口采用 multipart/form-data 格式；查询参数通过 URL 拼接传递，路径参数嵌入接口路径中。

• 响应格式：所有接口响应数据格式统一为 JSON，包含状态码（code）、提示信息（message）、响应数据（data）三部分，示例如下：

{

```
  "code": 200,
  "message": "操作成功",
  "data": {
    "userId": 1001,
    "username": "zhangsan",
    "nickname": "张三"
  }
}
```

• 状态码定义：遵循 HTTP 状态码语义，结合业务场景扩展，核心状态码包括：200（操作成功）、400（请求参数错误）、401（未认证/Token 失效）、403（权限不足）、404（资源不存在）、500（服务器内部错误）、503（服务暂时不可用）。

• 错误处理：接口报错时，响应体中“message”字段返回具体错误信息（如“参数 userId 不能为空”“Token 已过期，请重新登录”），便于前端定位问题；服务器内部错误时，隐藏详细错误堆栈，仅返回通用提示，详细错误信息记录至系统日志。

13.1.4 数据校验规范

• 请求参数校验：接口层对所有请求参数进行校验，包括必填项校验、数据类型校验、格式校验（如手机号、日期格式）、长度

校验、范围校验（如状态值枚举范围）；校验不通过时，返回400 错误，明确提示错误参数。

• 业务规则校验：接口层对核心业务场景进行规则校验，如“审批驳回时必须填写驳回意见”“文件上传大小不能超过 200MB”；校验不通过时，返回 400 错误，提示业务规则要求。

• 数据一致性校验：涉及数据更新、删除的接口，校验数据版本或状态，避免并发操作导致数据冲突；如“审批已通过的申请不能撤回”“已归档的文件不能修改”。

13.2 核心接口分类与功能说明

系统 API 接口按功能模块分为认证接口、用户管理接口、部门管理接口、角色权限接口、审批管理接口、文件管理接口、日志管理接口、系统配置接口八大类，核心接口功能如下：

13.2.1 认证接口

认证接口是系统身份校验与会话管理的核心入口，负责用户登录鉴权、Token 管理、密码操作等功能，确保接口访问的合法性与安全性，核心接口如下：

13.2.1.1 登录接口：POST /api/v1/auth/login

• 功能描述：用户通过用户名和密码完成身份校验，成功后获取系统访问 Token 及用户基础信息，支持账号状态、密码有效性校验。

• 请求头：Content-Type: application/json

• 请求体参数：

◦ username：字符串（必填），用户登录账号（6-20 位字母/数字组合）；

◦ password：字符串（必填），用户登录密码（符合系统密码复杂度要求）；

◦ clientInfo：对象（可选），客户端信息，包含 deviceModel（设备型号）、osVersion（操作系统版本）、browserType（浏览器类型），用于登录日志记录。

• 响应数据：

```
{
  "code": 200,
  "message": "登录成功",
  "data": {
    "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...",
// JWT 令牌
    "expireTime": "2024-06-20 15:30:45", // Token 过期时
间（精确到秒）
    "userInfo": {
      "userId": 1001,
      "username": "zhangsan",
      "nickname": "张三",
      "deptId": 201,
      "deptName": "市场部",
      "roleId": 3,
      "roleName": "审批员",
      "phone": "加密脱敏显示" // 敏感信息脱敏
    }
  }
}
```

- 异常响应：

◦ 400：参数错误（如用户名/密码为空、格式不正确）；

◦ 401：账号不存在、密码错误、账号已禁用/锁定；

◦ 500：服务器内部错误（如数据库连接异常）。

• 业务逻辑：

1. 校验用户名、密码参数完整性与格式；

2. 查询用户表，验证账号是否存在及状态是否为“启用”；

3. 校验密码哈希值与数据库存储值是否一致；

4. 检查账号是否因登录失败次数超限被锁定；

5. 生成 JWT Token（包含用户 ID、角色 ID、过期时间等信息，采用 HS256 加密）；

6. 记录登录日志（用户名、IP、设备信息、登录结果）；

7. 返回 Token、过期时间及脱敏后的用户基础信息。

13.2.1.2 退出登录接口：POST /api/v1/auth/logout

• 功能描述：用户主动退出登录，销毁当前会话 Token，更新登录日志中的退出时间。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（登录时获取的 JWT 令牌）

• 请求体参数：无

• 响应数据：

```
{
  "code": 200,
  "message": "退出成功",
  "data": null
}
```

• 异常响应：

◦ 401：Token 无效、已过期或未携带 Token；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 解析并验证请求头中的 Token 有效性；

2. 查找当前 Token 对应的登录日志记录，更新退出时间；

3. 将 Token 加入服务器黑名单（有效期内禁止再次使用）；

4. 返回退出成功响应。

13.2.1.3 Token 刷新接口：POST /api/v1/auth/refresh-token

• 功能描述：Token 即将过期时，用户无需重新登录，通过该接口获取新的有效 Token，保障业务操作连续性。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（即将过期的旧 Token）

• 请求体参数：无

• 响应数据：

```
{
  "code": 200,
  "message": "Token 刷新成功",
  "data": {
    "newToken":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...", // 新 JWT 令牌
    "expireTime": "2024-06-20 17:30:45" // 新 Token 过期
时间
  }
}
```

• 异常响应：

◦ 401：旧 Token 无效、已过期或未携带；

◦ 403：Token 已被拉黑（如用户已退出登录）；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 解析并验证旧 Token 的有效性（未过期、签名正确）；

2. 从旧 Token 中提取用户 ID、角色 ID 等核心信息；

3. 生成新的 JWT Token（沿用核心信息，更新过期时间）；

4. 将旧 Token 加入黑名单，新 Token 生效；

5. 返回新 Token 及过期时间。

13.2.1.4 密码修改接口：PUT /api/v1/auth/change-password

• 功能描述：用户登录后修改自身密码，支持旧密码校验、新密码复杂度校验，修改后即时生效。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}

• 请求体参数：

◦ oldPassword：字符串（必填），用户当前登录密码；

◦ newPassword：字符串（必填），新密码（需符合系统密码复杂度要求）；

◦ confirmPassword：字符串（必填），确认新密码（需与newPassword一致）。

• 响应数据：

```
{
  "code": 200,
  "message": "密码修改成功，请重新登录",
  "data": null
}
```

• 异常响应：

◦ 400：参数错误（如两次密码不一致、新密码不符合复杂度要

求）；

◦ 401：Token 无效、旧密码验证失败；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性，提取当前用户 ID；

2. 校验旧密码与数据库存储的密码哈希值是否一致；

3. 校验新密码与确认密码一致性，及新密码复杂度；

4. 计算新密码的 SHA-256 哈希值（含随机盐值），更新用户表密码字段；

5. 记录操作日志（用户 ID、操作类型“密码修改”、操作结果）；

6. 拉黑当前 Token，要求用户重新登录。

13.2.1.5 密码重置接口：POST /api/v1/auth/reset-password

• 功能描述：仅管理端用户可调用，用于重置指定用户的密码为系统初始密码，支持批量重置，重置后需提醒用户修改。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“用户管理”权限）

• 请求体参数：

◦ userIds：数组（必填），需重置密码的用户 ID 列表（如 [1001, 1002]）；

◦ initPassword：字符串（可选），自定义初始密码（未传则使用系统默认初始密码，需符合密码策略）。

• 响应数据：

{

```
  "code": 200,
  "message": "密码重置成功",
  "data": {
    "successIds": [1001, 1002], // 重置成功的用户 ID
    "failIds": [], // 重置失败的用户 ID（如用户不存在）
    "initPassword": "********" // 初始密码（脱敏显示，仅返回一次）
  }
}
```

- 异常响应：

◦ 400：参数错误（如 userIds 为空、自定义初始密码不符合复杂度）；

◦ 401：Token 无效或已过期；

◦ 403：当前用户无密码重置权限；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性，校验当前用户是否具备“用户管理”权限；

2. 校验 userIds 参数完整性，过滤不存在的用户 ID；

3. 生成初始密码（自定义或系统默认），计算哈希值；

4. 批量更新用户表中指定用户的密码字段，记录修改人 ID 与修改时间；

5. 记录操作日志（操作人 ID、操作类型“密码重置”、涉及用户 ID 列表）；

6. 返回重置结果及脱敏后的初始密码。

13.2.1.6 账号解锁接口：POST /api/v1/auth/unlock-account

• 功能描述：仅管理端用户可调用，用于解锁因登录失败次数超限被锁定的用户账号。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“用户管理”权限）

• 请求体参数：

◦ userId：整数（必填），被锁定的用户 ID；

◦ unlockReason：字符串（可选），解锁原因（如“用户误输密码导致锁定”）。

• 响应数据：

```
{
  "code": 200,
  "message": "账号解锁成功",
  "data": {
    "userId": 1001,
    "username": "zhangsan",
    "unlockTime": "2024-06-20 14:25:30"
  }
}
```

- 异常响应：

◦ 400：参数错误（如 userId 为空）；

◦ 401：Token 无效或已过期；

◦ 403：当前用户无账号解锁权限；

◦ 404：用户不存在或账号未锁定；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性，校验当前用户权限；

2. 查询用户表，确认用户存在且账号状态为“锁定”；

3. 更新用户表账号状态为“启用”，重置登录失败次数；

4. 记录操作日志（操作人 ID、操作类型“账号解锁”、用户 ID、解锁原因）；

5. 返回解锁成功响应及相关信息。

13.2.2 用户管理接口

用户管理接口面向管理端用户，提供用户账号的创建、查询、编辑、禁用/启用等功能，支持批量操作，核心接口如下：

13.2.2.1 创建用户接口：POST /api/v1/users

• 功能描述：管理端创建新用户账号，分配所属部门、角色，设置初始密码，支持字段校验与重复账号检测。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“用户创建”权限）

• 请求体参数：

◦ username：字符串（必填），登录账号（6-20 位字母/数字组合，唯一）；

◦ nickname：字符串（必填），用户昵称（1-30 位字符）；

◦ deptId：整数（必填），所属部门 ID（关联部门表）；

◦ roleId：整数（必填），角色 ID（关联角色表）；

◦ phone：字符串（可选），手机号（11 位数字，唯一）；

◦ initPassword：字符串（可选），初始密码（未传则使用系统默认，需符合密码策略）；

◦ status：整数（可选），账号状态（0-禁用、1-启用，默认 1）；

◦ remark：字符串（可选），备注信息（如“市场部新入职员工”）。

• 响应数据：

{

```
  "code": 200,
  "message": "用户创建成功",
  "data": {
    "userId": 1003,
    "username": "lisi",
    "nickname": "李四",
    "initPassword": "********" // 初始密码脱敏显示
  }
}
```

- 异常响应：

◦ 400：参数错误（如用户名格式不正确、手机号格式错误）；

◦ 401：Token 无效或已过期；

◦ 403：当前用户无创建用户权限；

◦ 409：用户名或手机号已存在；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与用户权限；

2. 校验所有请求参数的完整性、格式与唯一性（用户名、手机号）；

3. 生成初始密码，计算 SHA-256 哈希值（含盐值）；

4. 向用户表插入新用户记录，关联部门 ID 与角色 ID，记录创建人 ID 与创建时间；

5. 记录操作日志（操作人 ID、操作类型“创建用户”、新用户 ID）；

6. 返回创建结果及脱敏初始密码。

13.2.2.2 查询用户列表接口：GET /api/v1/users

• 功能描述：管理端查询系统用户列表，支持按部门、角色、状态、用户名等多条件筛选，支持分页与排序。

• 请求头：

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“用户查询”权限）

• 查询参数：

◦ deptId：整数（可选），按所属部门筛选；

◦ roleId：整数（可选），按角色筛选；

◦ status：整数（可选），按账号状态筛选（0-禁用、1-启用）；

◦ username：字符串（可选），按用户名模糊查询；

◦ pageNum：整数（必填），页码（默认 1）；

◦ pageSize：整数（必填），每页条数（默认 10，最大 50）；

◦ sortField：字符串（可选），排序字段（如“createTime”）；

◦ sortOrder：字符串（可选），排序方向（asc-升序、desc-降

序，默认 desc）。

- 响应数据：


```
{
  "code": 200,
  "message": "查询成功",
  "data": {
    "total": 120, // 总记录数
    "pageNum": 1,
    "pageSize": 10,
    "list": [
      {
        "userId": 1001,
        "username": "zhangsan",
        "nickname": "张三",
        "deptId": 201,
        "deptName": "市场部",
        "roleId": 3,
        "roleName": "审批员",
        "phone": "138****1234", // 脱敏显示
        "status": 1,
        "statusName": "启用",
```

```
        "lastLoginTime": "2024-06-19 09:30:15",
        "createTime": "2024-05-01 10:00:00"
      },
      // 更多用户记录...
    ]
  }
}
```


- 异常响应：

◦ 400：参数错误（如 pageNum/pageSize 非法）；

◦ 401：Token 无效或已过期；

◦ 403：当前用户无用户查询权限；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与用户权限；

2. 解析查询参数，构建多条件组合查询 SQL；

3. 执行分页查询，关联部门表、角色表获取部门名称、角色名称；

4. 对手机号等敏感信息进行脱敏处理；

5. 计算总记录数，返回分页结果；

6. 记录操作日志（操作人 ID、操作类型“查询用户列表”、筛选条件）。

13.2.2.3 查询用户详情接口：GET /api/v1/users/{userId}

• 功能描述：管理端查询指定用户的详细信息，全面覆盖基础信息、组织归属、角色权限、登录轨迹等核心维度，为用户管理与审计提供完整数据支撑。

• 请求头：

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“用户查询”权限）

• 路径参数：

◦ userId：整数（必填），用户唯一标识 ID，用于精准定位查询对象。

• 响应数据：

```
{
  "code": 200,
  "message": "查询成功",
  "data": {
    "baseInfo": {
      "userId": 1001,
      "username": "zhangsan",
      "nickname": "张三",
      "deptId": 201,
      "deptName": "市场部",
      "roleId": 3,
      "roleName": "审批员",
      "phone": "138****1234", // 手机号脱敏显示
      "status": 1,
      "statusName": "启用",
      "lastLoginTime": "2024-06-19 09:30:15",
```

```
  "lastLoginIp": "192.168.1.100",
  "lastLoginDevice": "Windows 11 Chrome 120.0",
  "createBy": 1000,
  "createByName": "系统管理员",
  "createTime": "2024-05-01 10:00:00",
  "updateBy": 1000,
  "updateByName": "系统管理员",
  "updateTime": "2024-06-01 14:20:30",
  "remark": "市场部合同审批负责人"
},
"rolePermInfo": {
  "roleId": 3,
  "roleName": "审批员",
  "permissions": [
    {
      "permId": 101,
      "permName": "查看待审批申请",
      "permKey": "seal:approve:pending:view"
    },
    {
      "permId": 102,
      "permName": "审批用章申请",
```

```
      "permKey": "seal:approve:deal"
    },
    {
      "permId": 103,
      "permName": "查询审批记录",
      "permKey": "seal:approve:record:view"
    }
    // 更多权限项...
  ]
},
"loginLogInfo": {
  "total": 156, // 累计登录次数
  "latestLogs": [
    {
      "loginTime": "2024-06-19 09:30:15",
      "loginIp": "192.168.1.100",
      "loginDevice": "Windows 11 Chrome 120.0",
      "loginLocation": "北京市朝阳区",
      "loginResult": "成功"
    },
    {
      "loginTime": "2024-06-18 16:45:22",
```

```
            "loginIp": "192.168.1.101",
            "loginDevice": "iPhone 14 iOS 16.5",
            "loginLocation": "北京市海淀区",
            "loginResult": "成功"
          }
          // 最新3条登录日志...
        ]
      }
    }
}
```


- 异常响应：

◦ 400：参数错误（如userId为空或非整数）；

◦ 401：Token无效、已过期或未携带Token；

◦ 403：当前用户无用户查询权限；

◦ 404：指定userId的用户不存在；

◦ 500：服务器内部错误（如数据库查询异常）。

- 业务逻辑：

1. 验证请求头中 Token 的有效性，解析操作人身份及权限；

2. 校验路径参数 userId 的合法性，确保为有效整数；

3. 从用户表查询基础信息，关联部门表、角色表获取部门名称、角色名称；

4. 从角色权限关联表、权限表查询该用户所属角色的所有权限项，组装角色权限信息；

5. 从登录日志表查询该用户的累计登录次数及最新 3 条登录记录，敏感信息（如 IP）按规则展示；

6. 对手机号等敏感数据进行脱敏处理，避免信息泄露；

7. 记录操作日志（操作人 ID、操作类型“查询用户详情”、目标用户 ID）；

8. 组装完整响应数据，返回给客户端。

13.2.2.4 编辑用户接口：PUT /api/v1/users/{userId}

• 功能描述：管理端修改指定用户的基础信息（如昵称、所属部门、角色、手机号）、账号状态（启用/禁用），支持部分字段更新，修改后即时生效。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“用户编辑”权限）

• 路径参数：

◦ userId：整数（必填），待编辑用户的唯一 ID。

• 请求体参数：

◦ nickname：字符串（可选），用户昵称（1-30 位字符）；

◦ deptId：整数（可选），新的所属部门 ID（关联部门表）；

◦ roleId：整数（可选），新的角色 ID（关联角色表）；

◦ phone：字符串（可选），手机号（11 位数字，需唯一）；

◦ status：整数（可选），账号状态（0-禁用、1-启用）；

◦ remark：字符串（可选），备注信息（如“调岗至销售部”）。

• 响应数据：

```
{
  "code": 200,
  "message": "用户编辑成功",
  "data": {
    "userId": 1001,
    "username": "zhangsan",
    "updateTime": "2024-06-20 15:10:25"
  }
}
```

• 异常响应：

◦ 400：参数错误（如手机号格式错误、状态值非法）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无用户编辑权限；

◦ 404：指定 userId 的用户不存在；

◦ 409：修改后的手机号已被其他用户占用；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性与操作人权限，解析操作人 ID；

2. 校验路径参数 userId 的合法性，查询用户是否存在；

3. 校验请求体参数（如手机号格式、状态值范围），若修改手机号需验证唯一性；

4. 仅更新请求体中传入的非空字段，保留未修改字段的原始值；

5. 若修改账号状态为“禁用”，同步检查该用户是否有未完成的审批任务，记录相关信息至操作日志；

6. 更新用户表中对应记录的修改人 ID、修改时间及相关字段值；

7. 记录操作日志（操作人 ID、操作类型“编辑用户”、目标用户 ID、修改前后字段对比）；

8. 返回编辑成功响应及关键信息。

13.2.2.5 启用/禁用用户接口：PATCH /api/v1/users/{userId}/status

• 功能描述：管理端单独控制指定用户的账号状态，支持批量启用/禁用，适用于用户离职、调岗等场景，操作更高效。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“用户状态管理”权限）

• 路径参数：

◦ userId：整数（必填），待操作用户的唯一 ID。

• 请求体参数：

◦ status：整数（必填），目标状态（0-禁用、1-启用）；

◦ operateReason：字符串（可选），操作原因（如“用户离职，禁用账号”）。

• 响应数据：


```
{
  "code": 200,
  "message": "用户账号已成功禁用",
  "data": {
    "userId": 1001,
    "username": "zhangsan",
    "status": 0,
```

```
    "statusName": "禁用",
    "operateTime": "2024-06-20 15:30:40"
  }
}
```


- 异常响应：

◦ 400：参数错误（如 status 值非法）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无用户状态管理权限；

◦ 404：指定 userId 的用户不存在；

◦ 409：用户当前状态与目标状态一致（如已禁用仍请求禁用）；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与操作人权限，解析操作人 ID；

2. 校验路径参数 userId 与请求体 status 的合法性，查询用户当前状态；

3. 若用户当前状态与目标状态一致，返回冲突错误；

4. 若目标状态为“禁用”，检查用户是否有未完成的用章申请或审批任务，记录相关任务 ID 至操作日志，便于后续交接；

5. 更新用户表中该用户的状态字段、修改人 ID 及修改时间；

6. 若状态改为“禁用”，同步拉黑该用户当前有效的登录 Token，强制退出登录；

7. 记录操作日志（操作人 ID、操作类型“修改用户状态”、目标用户 ID、原状态、目标状态、操作原因）；

8. 返回操作成功响应及状态变更信息。

13.2.2.6 批量操作用户接口：POST /api/v1/users/batch-operate

- 功能描述：管理端批量执行用户创建、编辑、启用/禁用、密

码重置操作，支持批量处理多个用户，提升管理效率，适用于批量入职、离职等场景。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理端账号 Token，需具备对应批量操作权限）

• 请求体参数：

◦ operateType：字符串（必填），批量操作类型（create-批量创建、update-批量编辑、status-批量修改状态、resetPwd-批量重置密码）；

◦ userList：数组（必填），待操作用户列表，不同操作类型对应不同参数结构：

```
// 批量创建参数示例
[
{
"username": "wangwu",
```

```
"nickname": "王五",
"deptId": 202,
"roleId": 2,
"phone": "139****4567",
"status": 1
}
// 更多用户...
]
// 批量修改状态参数示例
[
{
"userId": 1004,
"status": 0,
"operateReason": "离职"
}
// 更多用户...
]
```

- 响应数据：

```
{
  "code": 200,
  "message": "批量操作完成",
```

```
  "data": {
    "operateType": "status",
    "totalCount": 5, // 总操作数量
    "successCount": 4, // 成功数量
    "failCount": 1, // 失败数量
    "successList": [1004, 1005, 1006, 1007], // 成功操作的用户 ID/用户名
    "failList": [
      {
        "userId": 1008,
        "reason": "用户不存在"
      }
    ] // 失败详情
  }
}
```

• 异常响应：

◦ 400：参数错误（如 operateType 非法、userList 为空、参数格式不正确）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无对应批量操作权限；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性与操作人权限，根据 operateType 校验对应权限（如批量创建需“用户创建”权限）；

2. 校验 operateType 合法性及 userList 参数完整性、格式正确性；

3. 遍历 userList，按操作类型分别执行对应逻辑（创建、编辑、状态修改、密码重置），独立处理每个用户的操作结果，避免单个用户失败影响整体批量操作；

4. 记录每个用户的操作结果（成功/失败），失败时明确标注原因；

5. 批量记录操作日志（操作人 ID、操作类型“批量 XXX”、总操作数量、成功/失败详情）；

6. 汇总批量操作结果，返回给客户端。

13.2.2.7 导出用户列表接口：GET /api/v1/users/export

• 功能描述：管理端导出符合筛选条件的用户列表数据，支持Excel格式导出，包含用户基础信息、所属部门、角色、状态等核心字段，便于离线统计与存档。

• 请求头：

◦ Authorization: Bearer {token}（管理端账号Token，需具备“用户导出”权限）

• 查询参数：

◦ deptId：整数（可选），按所属部门筛选；

◦ roleId：整数（可选），按角色筛选；

◦ status：整数（可选），按账号状态筛选（0-禁用、1-启用）；

◦ username：字符串（可选），按用户名模糊查询；

◦ exportFields：字符串（可选），指定导出字段（如“userId,username,nickname,deptName”，未指定则导出全部字段）。

• 响应数据：

◦ 响应类型：application/vnd.openxmlformats-officedocument.spreadsheetml.sheet（Excel 文件）；

◦ 响应头：Content-Disposition: attachment; filename="用户列表_20240620.xlsx"（文件名含导出日期）。

• 异常响应：

◦ 400：参数错误（如 exportFields 字段不存在）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无用户导出权限；

◦ 500：服务器内部错误（如文件生成失败）。

• 业务逻辑：

1. 验证 Token 有效性与操作人权限；

2. 解析查询参数，构建筛选条件，查询符合条件的用户数据；

3. 若指定 exportFields，仅保留该字段列表中的字段，否则默认导出全部核心字段；

4. 将查询结果转换为 Excel 格式，设置表头、单元格格式，对手机号等敏感信息脱敏处理；

5. 生成 Excel 文件，设置响应头，触发客户端下载；

6. 记录操作日志（操作人 ID、操作类型“导出用户列表”、筛选条件、导出字段、导出时间）；

7. 若导出数据量过大（如超过 1000 条），异步生成文件并通过系统消息通知用户下载，避免同步请求超时。

13.2.3 部门管理接口

部门管理接口面向管理端用户，提供部门的创建、查询、编辑、删除等功能，支持多级部门架构维护，适配复杂组织架构管理需求，核心接口如下：

13.2.3.1 创建部门接口：POST /api/v1/depts

• 功能描述：管理端创建新部门，支持设置上级部门以构建多级组织架构，严格校验部门名称与代号的唯一性，确保组织架构数据规范。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“部门创建”权限）

• 请求体参数：

◦ deptName：字符串（必填），部门名称（1-50 位字符，支持中文、字母、数字及常用符号，同一上级部门下名称不可重复）；

◦ deptCode：字符串（必填），部门代号（1-20 位字母/数字组合，全局唯一，用于审批编号生成、数据分类等场景）；

◦ parentId：整数（可选），上级部门 ID（关联部门表，顶级部门父 ID 为 0，默认值为 0，支持多级嵌套）；

◦ leaderId：整数（可选），部门负责人 ID（关联用户表，需为系统已存在的用户账号）；

◦ sort：整数（可选），部门排序权重（默认值为 0，数值越小在列表中排序越靠前，支持正负整数）；

◦ remark：字符串（可选），部门备注信息（如“负责华东区域产品销售与客户维护”，长度不超过 200 位字符）。

• 响应数据：


```
{
  "code": 200,
  "message": "部门创建成功",
  "data": {
    "deptId": 203,
```

```
    "deptName": "华东销售部",
    "deptCode": "SALES-EAST",
    "parentId": 200,
    "parentName": "销售中心",
    "leaderId": 1005,
    "leaderName": "赵六",
    "sort": 10,
    "createBy": 1000,
    "createByName": "系统管理员",
    "createTime": "2024-06-20 16:05:30"
  }
}
```


- 异常响应：

◦ 400：参数错误（如部门名称为空、代号格式非法、上级部门 ID 不存在）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无部门创建权限；

◦ 409：部门名称在同一上级部门下已存在，或部门代号全局重

复；

◦ 500：服务器内部错误（如数据库插入失败）。

• 业务逻辑：

1. 验证请求头 Token 有效性，解析操作人身份及权限；

2. 校验请求体参数完整性与格式，若传入 parentId 则验证上级部门是否存在；

3. 校验部门名称唯一性（同一 parentId 下无重复）与部门代号全局唯一性；

4. 若传入 leaderId，验证该用户是否存在且状态为“启用”；

5. 向部门表插入新部门记录，关联上级部门 ID、负责人 ID，记录创建人 ID 与创建时间；

6. 记录操作日志（操作人 ID、操作类型“创建部门”、新部门 ID、部门名称、上级部门 ID）；

7. 组装响应数据，返回新部门完整信息（含上级部门名称、负责人名称）。

13.2.3.2 查询部门列表接口：GET /api/v1/depts

• 功能描述：管理端查询系统部门列表，支持按上级部门、负责人、部门名称/代号模糊查询，支持树形结构与扁平结构两种返回格式，适配不同管理场景。

• 请求头：

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“部门查询”权限）

• 查询参数：

◦ parentId：整数（可选），按上级部门 ID 筛选（传入 0 查询所有顶级部门）；

◦ leaderId：整数（可选），按部门负责人 ID 筛选；

◦ keyword：字符串（可选），按部门名称或部门代号模糊查询；

◦ returnType：字符串（可选），返回格式（tree-树形结构、list-扁平结构，默认 tree）；

◦ sortField：字符串（可选），排序字段（如“sort”“createTime”，默认“sort”）；

◦ sortOrder：字符串（可选），排序方向（asc-升序、desc-降序，默认 asc）。

• 响应数据（树形结构示例）：


```
{
  "code": 200,
  "message": "查询成功",
  "data": [
    {
      "deptId": 200,
      "deptName": "销售中心",
      "deptCode": "SALES-CENTER",
      "parentId": 0,
      "parentName": "顶级部门",
      "leaderId": 1003,
```

```
"leaderName": "张三",
"sort": 5,
"createTime": "2024-05-01 10:00:00",
"children": [
  {
    "deptId": 203,
    "deptName": "华东销售部",
    "deptCode": "SALES-EAST",
    "parentId": 200,
    "parentName": "销售中心",
    "leaderId": 1005,
    "leaderName": "赵六",
    "sort": 10,
    "createTime": "2024-06-20 16:05:30",
    "children": []
  },
  {
    "deptId": 204,
    "deptName": "华南销售部",
    "deptCode": "SALES-SOUTH",
    "parentId": 200,
    "parentName": "销售中心",
```

```
            "leaderId": 1006,
            "leaderName": "孙七",
            "sort": 20,
            "createTime": "2024-06-20 16:10:20",
            "children": []
          }
        ]
      }
      // 更多部门节点...
    ]
}
```


- 异常响应：

◦ 400：参数错误（如 returnType 值非法）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无部门查询权限；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与操作人权限；

2. 解析查询参数，构建筛选条件（上级部门、负责人、关键词模糊匹配）；

3. 按筛选条件查询部门表数据，关联用户表获取负责人名称；

4. 若 returnType 为“tree”，按 parentId 层级递归组装树形结构；若为“list”，直接返回扁平列表；

5. 按 sortField 与 sortOrder 对部门数据排序；

6. 记录操作日志（操作人 ID、操作类型“查询部门列表”、筛选条件、返回格式）；

7. 返回查询结果。

13.2.3.3 查询部门详情接口：GET /api/v1/depts/{deptId}

• 功能描述：管理端查询指定部门的详细信息，包括基础配置、上级部门关联、负责人信息及下属部门列表，为部门管理提供完

整数据视图。

• 请求头：

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“部门查询”权限）

• 路径参数：

◦ deptId：整数（必填），部门唯一标识 ID。

• 响应数据：


```
{
  "code": 200,
  "message": "查询成功",
  "data": {
    "baseInfo": {
      "deptId": 203,
      "deptName": "华东销售部",
      "deptCode": "SALES-EAST",
      "parentId": 200,
      "parentName": "销售中心",
```

```
    "leaderId": 1005,
    "leaderName": "赵六",
    "leaderPhone": "139****4567", // 负责人手机号脱敏
    "sort": 10,
    "createBy": 1000,
    "createByName": "系统管理员",
    "createTime": "2024-06-20 16:05:30",
    "updateBy": 1000,
    "updateByName": "系统管理员",
    "updateTime": "2024-06-20 16:05:30",
    "remark": "负责华东区域产品销售与客户维护"
  },
  "subDeptList": [
    {
      "deptId": 205,
      "deptName": "上海销售组",
      "deptCode": "SALES-SH",
      "sort": 5
    }
    // 下属部门列表...
  ],
  "userCountInfo": {
```

```
        "totalUser": 25, // 部门下总用户数
        "enabledUser": 23, // 启用状态用户数
        "disabledUser": 2 // 禁用状态用户数
      }
    }
}
```


- 异常响应：

◦ 400：参数错误（如 deptId 为空或非整数）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无部门查询权限；

◦ 404：指定 deptId 的部门不存在；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与操作人权限；

2. 校验路径参数 deptId 合法性，查询部门基础信息；

3. 关联查询上级部门名称、负责人详细信息（脱敏手机号）；

4. 查询该部门下的下属部门列表（parentId=当前 deptId）；

5. 统计该部门及下属部门的用户总数、启用/禁用用户数；

6. 记录操作日志（操作人 ID、操作类型“查询部门详情”、目标部门 ID）；

7. 组装完整响应数据并返回。

13.2.3.4 编辑部门接口：PUT /api/v1/depts/{deptId}

• 功能描述：管理端修改指定部门的基础信息，包括部门名称、代号、上级部门、负责人、排序等，支持部分字段更新，确保修改后数据唯一性。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“部门编辑”权限）

• 路径参数：

◦ deptId：整数（必填），待编辑部门的唯一 ID。

• 请求体参数：

◦ deptName：字符串（可选），新部门名称（1-50 位字符，同一上级部门下需唯一）；

◦ deptCode：字符串（可选），新部门代号（1-20 位字母/数字组合，全局需唯一）；

◦ parentId：整数（可选），新上级部门 ID（不可设置为自身或下属部门 ID）；

◦ leaderId：整数（可选），新部门负责人 ID（关联用户表，可为空）；

◦ sort：整数（可选），新排序权重；

◦ remark：字符串（可选），新备注信息。

• 响应数据：

```
{
  "code": 200,
  "message": "部门编辑成功",
  "data": {
    "deptId": 203,
    "deptName": "华东大区销售部",
    "updateTime": "2024-06-20 16:30:45"
  }
}
```

• 异常响应：

◦ 400：参数错误（如上级部门 ID 为自身 ID、负责人 ID 不存在）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无部门编辑权限；

◦ 404：指定 deptId 的部门不存在；

◦ 409：修改后的部门名称/代号与其他部门冲突；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性与操作人权限，解析操作人 ID；

2. 校验路径参数 deptId 合法性，查询部门当前信息；

3. 校验请求体参数（如 parentId 不可为自身或下属部门 ID、名称/代号唯一性）；

4. 仅更新传入的非空字段，保留未修改字段原始值；

5. 若修改负责人 ID，验证目标用户是否存在且状态为“启用”；

6. 更新部门表对应记录的修改人 ID、修改时间及相关字段；

7. 记录操作日志（操作人 ID、操作类型“编辑部门”、目标部门 ID、修改前后字段对比）；

8. 返回编辑成功响应。

13.2.3.5 删除部门接口：DELETE /api/v1/depts/{deptId}

• 功能描述：管理端删除指定部门，仅支持删除无下属部门、无关联用户的空部门，避免数据关联冲突，保障组织架构数据一致性。

• 请求头：

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“部门删除”权限）

• 路径参数：

◦ deptId：整数（必填），待删除部门的唯一 ID。

• 响应数据：

```
{
  "code": 200,
  "message": "部门删除成功",
  "data": {
    "deptId": 205,
    "deptName": "上海销售组"
  }
}
```


- 异常响应：

◦ 400：参数错误（如 deptId 为空或非整数）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无部门删除权限；

◦ 404：指定 deptId 的部门不存在；

◦ 409：部门下存在下属部门或关联用户，无法删除；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与操作人权限；

2. 校验路径参数 deptId 合法性，查询部门是否存在；

3. 检查该部门下是否存在下属部门（parentId=当前 deptId 的部门）；

4. 检查该部门是否关联用户（用户表中 deptId=当前 deptId 的用户）；

5. 若存在下属部门或关联用户，返回冲突错误；

6. 执行部门表删除操作，记录操作人 ID 与删除时间（逻辑删除或物理删除，根据配置）；

7. 记录操作日志（操作人 ID、操作类型“删除部门”、目标部门 ID、部门名称）；

8. 返回删除成功响应。

13.2.3.6 导出部门列表接口：GET /api/v1/depts/export

• 功能描述：管理端导出符合筛选条件的部门列表数据，支持Excel格式，包含部门基础信息、上级部门、负责人、用户统计等字段，便于离线存档与分析。

• 请求头：

◦ Authorization: Bearer {token}（管理端账号Token，需具备“部门导出”权限）

• 查询参数：

◦ parentId：整数（可选），按上级部门筛选；

◦ keyword：字符串（可选），按部门名称/代号模糊查询；

◦ exportFields：字符串（可选），指定导出字段（如“deptId,deptName,deptCode,leaderName”，未指定则导出全部字段）。

• 响应数据：

◦ 响应类型：application/vnd.openxmlformats-officedocument.spreadsheetml.sheet（Excel 文件）；

◦ 响应头：Content-Disposition: attachment; filename="部门列表_20240620.xlsx"。

• 异常响应：

◦ 400：参数错误（如 exportFields 字段不存在）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无部门导出权限；

◦ 500：服务器内部错误（如文件生成失败）。

• 业务逻辑：

1. 验证 Token 有效性与操作人权限；

2. 解析查询参数，构建筛选条件，查询符合条件的部门数据；

3. 关联查询上级部门名称、负责人名称、用户统计信息；

4. 按指定 exportFields 筛选导出字段，默认导出全部核心字段；

5. 生成 Excel 文件，设置表头与单元格格式，确保数据展示清晰；

6. 触发客户端下载，记录操作日志（操作人 ID、操作类型“导出部门列表”、筛选条件、导出时间）；

7. 大数据量导出时采用异步生成机制，通过系统消息通知用户下载。

13.2.4 角色权限接口

角色权限接口面向管理端用户，提供角色的创建、查询、编辑、删除及权限分配功能，基于 RBAC 模型实现权限的精细化管控，支持角色与权限的灵活关联，核心接口如下：

13.2.4.1 创建角色接口：POST /api/v1/roles

• 功能描述：管理端创建自定义角色，设置角色名称、描述及状态，为后续权限分配奠定基础，支持角色名称唯一性校验。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“角色创建”权限）

• 请求体参数：

◦ roleName：字符串（必填），角色名称（1-30 位字符，全局唯一，如“法务审批员”“部门管理员”）；

◦ roleDesc：字符串（可选），角色描述（详细说明角色的权限范围与适用场景，长度不超过 200 位字符）；

◦ status：整数（可选），角色状态（0-禁用、1-启用，默认 1，禁用后关联该角色的用户无法使用对应权限）；

◦ sort：整数（可选），角色排序权重（默认 0，数值越小在列表中排序越靠前）。

• 响应数据：


```
{
  "code": 200,
  "message": "角色创建成功",
  "data": {
    "roleId": 6,
    "roleName": "法务审批员",
    "roleDesc": "负责合同类用章申请的法务审核",
    "status": 1,
    "createBy": 1000,
    "createByName": "系统管理员",
    "createTime": "2024-06-20 17:00:15"
  }
}
```


• 异常响应：

◦ 400：参数错误（如角色名称为空、长度超限）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无角色创建权限；

◦ 409：角色名称已存在；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性与操作人权限，解析操作人 ID；

2. 校验请求体参数完整性与格式，重点校验角色名称唯一性；

3. 向角色表插入新角色记录，记录创建人 ID、创建时间及相关配置；

4. 记录操作日志（操作人 ID、操作类型“创建角色”、新角色 ID、角色名称）；

5. 返回创建成功响应及角色核心信息。

13.2.4.2 查询角色列表接口：GET /api/v1/roles

• 功能描述：管理端查询系统所有角色列表，支持按角色名称模糊查询、按状态筛选，支持分页与排序，便于角色管理与检索。

• 请求头：

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“角色查询”权限）

• 查询参数：

◦ roleName：字符串（可选），按角色名称模糊查询；

◦ status：整数（可选），按角色状态筛选（0-禁用、1-启用）；

◦ pageNum：整数（必填），页码（默认 1）；

◦ pageSize：整数（必填），每页条数（默认 10，最大 50）；

◦ sortField：字符串（可选），排序字段（如“sort”“createTime”，默认“sort”）；

◦ sortOrder：字符串（可选），排序方向（asc-升序、desc-降序，默认 asc）。

• 响应数据：

```
{
  "code": 200,
  "message": "查询成功",
  "data": {
    "total": 8,
    "pageNum": 1,
    "pageSize": 10,
    "list": [
      {
        "roleId": 1,
        "roleName": "系统管理员",
        "roleDesc": "具备系统所有操作权限",
        "status": 1,
        "statusName": "启用",
        "userCount": 2, // 关联该角色的用户数量
        "createTime": "2024-05-01 10:00:00"
      },
      {
```

```
        "roleId": 6,
        "roleName": "法务审批员",
        "roleDesc": "负责合同类用章申请的法务审核",
        "status": 1,
        "statusName": "启用",
        "userCount": 3,
        "createTime": "2024-06-20 17:00:15"
      }
      // 更多角色记录...
    ]
  }
}
```


- 异常响应：

◦ 400：参数错误（如 pageNum/pageSize 非法）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无角色查询权限；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性与操作人权限；

2. 解析查询参数，构建筛选条件（名称模糊匹配、状态筛选）；

3. 执行分页查询，统计每个角色关联的用户数量；

4. 按指定排序字段与方向对角色列表排序；

5. 记录操作日志（操作人 ID、操作类型“查询角色列表”、筛选条件）；

6. 返回分页查询结果。

13.2.4.3 查询角色详情接口：GET /api/v1/roles/{roleId}

• 功能描述：管理端查询指定角色的详细信息，包括基础配置、关联的权限列表及关联用户数量，为权限调整与角色管理提供完整视图。

• 请求头：

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“角色查询”权限）

• 路径参数：

◦ roleId：整数（必填），角色唯一标识 ID。

• 响应数据：


```
{
  "code": 200,
  "message": "查询成功",
  "data": {
    "baseInfo": {
      "roleId": 6,
      "roleName": "法务审批员",
      "roleDesc": "负责合同类用章申请的法务审核",
      "status": 1,
      "statusName": "启用",
      "sort": 10,
      "createBy": 1000,
      "createByName": "系统管理员",
```

```
    "createTime": "2024-06-20 17:00:15",
    "updateBy": 1000,
    "updateByName": "系统管理员",
    "updateTime": "2024-06-20 17:00:15"
  },
  "permList": [
    {
      "permId": 105,
      "permName": "查看合同类待审批申请",
      "permKey": "seal:approve:contract:pending:view",
      "permType": 1,
      "permTypeName": "按钮权限"
    },
    {
      "permId": 106,
      "permName": "审核合同类用章申请",
      "permKey": "seal:approve:contract:deal",
      "permType": 1,
      "permTypeName": "按钮权限"
    }
    // 更多关联权限项...
  ],
```

```
    "userCount": 3 // 关联该角色的用户总数
  }
}
```

- 异常响应：

◦ 400：参数错误（如 roleId 为空或非整数）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无角色查询权限；

◦ 404：指定 roleId 的角色不存在；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与操作人权限；

2. 校验路径参数 roleId 合法性，查询角色基础信息；

3. 关联角色权限关联表、权限表，查询该角色的所有关联权限

项，包含权限名称、标识、类型等；

4. 统计关联该角色的用户总数；

5. 记录操作日志（操作人 ID、操作类型“查询角色详情”、目标角色 ID）；

6. 组装完整响应数据并返回。

13.2.4.4 编辑角色接口：PUT /api/v1/roles/{roleId}

• 功能描述：管理端修改指定角色的基础信息，包括角色名称、描述、状态、排序，支持部分字段更新，确保角色名称唯一性。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“角色编辑”权限）

• 路径参数：

◦ roleId：整数（必填），待编辑角色的唯一 ID。

• 请求体参数：

◦ roleName：字符串（可选），新角色名称（1-30 位字符，全局唯一）；

◦ roleDesc：字符串（可选），新角色描述；

◦ status：整数（可选），新角色状态（0-禁用、1-启用）；

◦ sort：整数（可选），新排序权重。

• 响应数据：


```
{
  "code": 200,
  "message": "角色编辑成功",
  "data": {
    "roleId": 6,
    "roleName": "合同法务审批员",
    "updateTime": "2024-06-20 17:20:30"
```

```
  }
}
```

- 异常响应：

◦ 400：参数错误（如角色名称长度超限）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无角色编辑权限；

◦ 404：指定 roleId 的角色不存在；

◦ 409：修改后的角色名称与其他角色冲突；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与操作人权限，解析操作人 ID；

2. 校验路径参数 roleId 合法性，查询角色当前信息；

3. 校验请求体参数，若修改角色名称需验证全局唯一性；

4. 仅更新传入的非空字段，保留未修改字段原始值；

5. 若修改角色状态为“禁用”，同步记录关联用户的权限失效情况至操作日志；

6. 更新角色表对应记录的修改人 ID、修改时间及相关字段；

7. 记录操作日志（操作人 ID、操作类型“编辑角色”、目标角色 ID、修改前后字段对比）；

8. 返回编辑成功响应。

13.2.4.5 分配权限接口：POST /api/v1/roles/{roleId}/permissions

• 功能描述：管理端为指定角色分配权限，支持批量添加或替换权限，实现角色与权限的灵活绑定，权限分配后即时生效。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“权限分配”权限）

• 路径参数：

◦ roleId：整数（必填），待分配权限的角色 ID。

• 请求体参数：

◦ permIds：数组（必填），权限 ID 列表（如[105, 106, 107]，需为系统已存在的权限 ID）；

◦ operateType：字符串（可选），操作类型（add-追加权限、replace-替换权限，默认 replace）。

• 响应数据：

```
{
  "code": 200,
  "message": "权限分配成功",
  "data": {
```

```
    "roleId": 6,
    "roleName": "合同法务审批员",
    "permCount": 5, // 分配后该角色的总权限数
    "operateType": "replace"
  }
}
```


- 异常响应：

◦ 400：参数错误（如 permIds 为空、权限 ID 不存在）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无权限分配权限；

◦ 404：指定 roleId 的角色不存在；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与操作人权限；

2. 校验路径参数 roleId 与请求体 permIds 的合法性，确保所有权限 ID 存在；

3. 若 operateType 为“replace”，先删除该角色原有的所有权限关联记录；若为“add”，跳过删除步骤；

4. 批量插入新的角色-权限关联记录至角色权限关联表；

5. 统计分配后该角色的总权限数；

6. 记录操作日志（操作人 ID、操作类型“分配权限”、目标角色 ID、权限 ID 列表、操作类型）；

7. 返回权限分配成功响应。

13.2.4.6 删除角色接口：DELETE /api/v1/roles/{roleId}

• 功能描述：管理端删除指定角色，仅支持删除无关联用户的角色，避免权限关联冲突，保障权限体系稳定性。

• 请求头：

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“角色删除”权限）

• 路径参数：

◦ roleId：整数（必填），待删除角色的唯一 ID。

• 响应数据：


```
{
  "code": 200,
  "message": "角色删除成功",
  "data": {
    "roleId": 7,
    "roleName": "临时审批员"
  }
}
```


• 异常响应：

◦ 400：参数错误（如 roleId 为空或非整数）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无角色删除权限；

◦ 404：指定 roleId 的角色不存在；

◦ 409：角色已关联用户，无法删除；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性与操作人权限；

2. 校验路径参数 roleId 合法性，查询角色是否存在；

3. 检查该角色是否关联用户（用户表中 roleId=当前 roleId 的用户）；

4. 若存在关联用户，返回冲突错误；

5. 先删除该角色在角色权限关联表中的所有权限关联记录；

6. 再删除角色表中的该角色记录；

7. 记录操作日志（操作人 ID、操作类型“删除角色”、目标角色 ID、角色名称）；

8. 返回删除成功响应。

13.2.4.7 查询权限列表接口：GET /api/v1/permissions

• 功能描述：管理端查询系统所有权限项列表，支持按权限名称、权限类型、上级权限筛选，支持树形结构与扁平结构返回，清晰展示权限层级关系，为角色权限分配提供直观选择依据。

• 请求头：

◦ Authorization: Bearer {token}（管理端账号 Token，需具备“权限查询”权限）

• 查询参数：

◦ permName：字符串（可选），按权限名称模糊查询（如“审批”“申请”）；

◦ permType：整数（可选），按权限类型筛选（0-菜单权限、1-按钮权限、2-接口权限）；

◦ parentId：整数（可选），按上级权限 ID 筛选（传入 0 查询所有顶级权限）；

◦ returnType：字符串（可选），返回格式（tree-树形结构、list-扁平结构，默认 tree）；

◦ sortField：字符串（可选），排序字段（如“permId”“sort”，默认“permId”）；

◦ sortOrder：字符串（可选），排序方向（asc-升序、desc-降序，默认 asc）。

• 响应数据（树形结构示例）：


```
{
  "code": 200,
  "message": "查询成功",
  "data": [
    {
      "permId": 100,
```

```
"permName": "用章申请管理",
"permKey": "seal:apply:manage",
"permType": 0,
"permTypeName": "菜单权限",
"parentId": 0,
"sort": 10,
"children": [
  {
    "permId": 101,
    "permName": "提交用章申请",
    "permKey": "seal:apply:submit",
    "permType": 1,
    "permTypeName": "按钮权限",
    "parentId": 100,
    "sort": 1
  },
  {
    "permId": 102,
    "permName": "查询我的申请",
    "permKey": "seal:apply:my:view",
    "permType": 1,
    "permTypeName": "按钮权限",
```

```
      "parentId": 100,
      "sort": 2
    },
    {
      "permId": 103,
      "permName": "撤回用章申请",
      "permKey": "seal:apply:withdraw",
      "permType": 1,
      "permTypeName": "按钮权限",
      "parentId": 100,
      "sort": 3
    }
  ]
},
{
  "permId": 200,
  "permName": "审批管理",
  "permKey": "seal:approve:manage",
  "permType": 0,
  "permTypeName": "菜单权限",
  "parentId": 0,
  "sort": 20,
```

```
  "children": [
    {
      "permId": 201,
      "permName": "查看待审批申请",
      "permKey": "seal:approve:pending:view",
      "permType": 1,
      "permTypeName": "按钮权限",
      "parentId": 200,
      "sort": 1
    },
    {
      "permId": 202,
      "permName": "审批用章申请",
      "permKey": "seal:approve:deal",
      "permType": 1,
      "permTypeName": "按钮权限",
      "parentId": 200,
      "sort": 2
    }
  ]
}
// 更多权限节点...
```

]
}

- 异常响应：

◦ 400：参数错误（如 permType 值非法、returnType 格式错误）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无权限查询权限；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与操作人权限；

2. 解析查询参数，构建筛选条件（名称模糊匹配、类型筛选、上级权限筛选）；

3. 按筛选条件查询权限表数据，获取所有符合条件的权限项；

4. 若 returnType 为“tree”，按 parentId 层级递归组装树形结构，体现权限父子关联；若为“list”，直接返回扁平列表；

5. 按 sortField 与 sortOrder 对权限数据排序，确保展示顺序一致；

6. 记录操作日志（操作人 ID、操作类型“查询权限列表”、筛选条件、返回格式）；

7. 返回查询结果。

13.2.5 审批管理接口

审批管理接口覆盖用章申请提交、审批处理、状态查询、记录追溯等核心业务流程，支持普通用户、审批人、管理员等不同角色操作，核心接口如下：

13.2.5.1 提交用章申请接口：POST /api/v1/approvals

• 功能描述：普通用户发起用章申请，填写申请信息、上传申请材料，系统自动生成唯一审批编号，触发审批流程推送，支持表单校验与文件上传校验。

• 请求头：

◦ Content-Type: multipart/form-data（含文件上传）

◦ Authorization: Bearer {token}（普通用户 Token，需具备“提交用章申请”权限）

• 请求参数（FormData 格式）：

◦ title：字符串（必填），申请标题（10-50 位字符，如“XX 项目合作协议盖章申请”）；

◦ deptId：整数（必填），申请所属部门 ID（关联部门表，默认当前用户所属部门）；

◦ purpose：整数（必填），用章用途（关联数据字典表，如 0-合同签署、1-公文用印）；

◦ fileType：字符串（必填），申请材料文件类型组合（如“Word,PDF,图片”）；

◦ remark：字符串（必填），申请说明（不少于 50 位字符，描述用章背景、文件数量等）；

◦ phone：字符串（必填），申请人联系方式（11 位手机号）；

◦ urgentLevel：整数（可选），紧急程度（0-普通、1-紧急、2-特急，默认 0）；

◦ planSealTime：字符串（可选），预计用章时间（日期格式“YYYY-MM-DD”）；

◦ ext1/ext2：字符串（可选），扩展字段（如项目编号、合同金额，根据系统配置启用）；

◦ files：文件数组（必填），申请材料文件（支持 JPG、PNG、Word、PDF 等格式，单个文件≤200MB，最多 10 个文件）。

• 响应数据：


```
{
  "code": 200,
  "message": "申请提交成功",
  "data": {
```

```
    "approvalId": 5001,
    "approvalNo": "2024-DEP01-00001",
    "status": 0,
    "statusName": "待审批",
    "submitTime": "2024-06-21 09:15:30",
    "nextNodeName": "部门负责人审批"
  }
}
```


• 异常响应：

◦ 400：参数错误（如标题长度不足、手机号格式错误、文件格式/大小超限）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无提交用章申请权限；

◦ 500：服务器内部错误（如数据库插入失败、文件上传失败）。

• 业务逻辑：

1. 验证 Token 有效性与用户权限，解析申请人 ID；

2. 校验所有请求参数完整性与格式，包括表单字段校验（如手机号、申请说明长度）与文件校验（格式、大小、数量）；

3. 根据用章用途（purpose）匹配对应的审批流程，确定首个审批节点；

4. 生成唯一审批编号（按系统配置规则，如“年份-部门代号-流水号”）；

5. 向审批表插入申请记录，关联申请人 ID、部门 ID、用章用途等信息，记录提交时间、设备信息、IP 地址；

6. 上传申请材料文件至服务器指定目录，生成文件元数据（名称、路径、哈希值等），插入文件表并关联当前审批 ID；

7. 推送审批任务至首个审批节点的审批人（如部门负责人），触发待办提醒；

8. 记录操作日志（操作人 ID、操作类型“提交用章申请”、审批编号、申请标题）；

9. 返回申请成功响应及核心信息（审批 ID、审批编号、当前状态、下一审批节点）。

13.2.5.2 查询我的申请列表接口：GET /api/v1/approvals/my

• 功能描述：普通用户查询自己发起的所有用章申请列表，支持按申请状态、用章用途、时间范围筛选，支持分页与排序，便于跟踪申请进度。

• 请求头：

◦ Authorization: Bearer {token}（普通用户 Token）

• 查询参数：

◦ status：整数（可选），申请状态（0-待审批、1-审批中、2-已通过、3-已驳回等）；

◦ purpose：整数（可选），用章用途（关联数据字典表）；

◦ startTime：字符串（可选），申请开始时间（日期格式“YYYY-MM-DD”）；

◦ endTime：字符串（可选），申请结束时间（日期格式“YYYY-MM-DD”）；

◦ keyword：字符串（可选），按申请标题/审批编号模糊查询；

◦ pageNum：整数（必填），页码（默认 1）；

◦ pageSize：整数（必填），每页条数（默认 10，最大 50）；

◦ sortField：字符串（可选），排序字段（如“createTime”“approvalNo”，默认“createTime”）；

◦ sortOrder：字符串（可选），排序方向（desc-降序、asc-升序，默认 desc）。

• 响应数据：


```
{
  "code": 200,
  "message": "查询成功",
  "data": {
    "total": 12,
```

```
    "pageNum": 1,
    "pageSize": 10,
    "list": [
      {
        "approvalId": 5001,
        "approvalNo": "2024-DEP01-00001",
        "title": "XX 项目合作协议盖章申请",
        "deptName": "市场部",
        "purposeName": "合同签署",
        "urgentLevelName": "普通",
        "status": 1,
        "statusName": "审批中",
        "submitTime": "2024-06-21 09:15:30",
        "currentNodeName": "法务审核",
        "fileCount": 3 // 申请材料文件数量
      },
      // 更多申请记录...
    ]
  }
}
```

- 异常响应：

◦ 400：参数错误（如日期格式错误、pageNum/pageSize 非法）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性，解析当前申请人 ID；

2. 解析查询参数，构建筛选条件（状态、用途、时间范围、关键词模糊匹配）；

3. 按“申请人 ID=当前用户 ID”+筛选条件查询审批表数据，关联部门表、数据字典表获取部门名称、用途名称、紧急程度名称；

4. 统计每个申请的材料文件数量，关联文件表查询；

5. 确定每个申请的当前审批节点名称，展示审批进度；

6. 执行分页查询，按指定排序字段与方向排序；

7. 记录操作日志（操作人 ID、操作类型“查询我的申请”、筛选条件）；

8. 返回分页查询结果。

13.2.5.3 查询申请详情接口：GET /api/v1/approvals/{approvalId}

• 功能描述：用户查询指定用章申请的详细信息，包括申请基础信息、审批流转记录、上传文件列表，支持申请人、审批人、管理员等不同角色查看（按权限控制可见范围），为申请跟踪、审批决策、记录追溯提供完整数据支撑。

• 请求头：

◦ Authorization: Bearer {token}（用户 Token，需具备对应查看权限）

• 路径参数：

◦ approvalId：整数（必填），申请唯一标识 ID。

• 响应数据：

```
{
  "code": 200,
  "message": "查询成功",
  "data": {
    "baseInfo": {
      "approvalId": 5001,
      "approvalNo": "2024-DEP01-00001",
      "title": "XX 项目合作协议盖章申请",
      "deptId": 201,
      "deptName": "市场部",
      "applyUserId": 1002,
      "applyUserName": "李四",
      "applyUserPhone": "138****1234", // 脱敏显示
      "purpose": 0,
      "purposeName": "合同签署",
      "fileType": "Word,PDF,图片",
      "remark": "XX 项目为公司重点合作项目，需盖章的协议共 3 份，分别为合作协议正文、补充协议、附件清单，申请紧急处理。",
```

```
    "urgentLevel": 0,
    "urgentLevelName": "普通",
    "planSealTime": "2024-06-25",
    "status": 1,
    "statusName": "审批中",
    "submitTime": "2024-06-21 09:15:30",
    "submitDevice": "Windows 11 Chrome 120.0",
    "submitIp": "192.168.1.102",
    "ext1": "XM202406001", // 扩展字段（项目编号）
    "ext2": "500万元" // 扩展字段（合同金额）
  },
  "fileList": [
    {
      "fileId": 10001,
      "fileName": "合作协议正文.docx",
      "fileType": "application/vnd.openxmlformats-officedocument.wordprocessingml.document",
      "fileSize": 2097152, // 字节数（2MB）
      "fileSizeStr": "2.0MB", // 人性化显示
      "fileSource": 0,
      "fileSourceName": "申请材料",
      "uploadTime": "2024-06-21 09:15:25",
```

```
      "uploadUserName": "李四",
      "fileHash": "e10adc3949ba59abbe56e057f20f883e"
    },
    {
      "fileId": 10002,
      "fileName": "补充协议.pdf",
      "fileType": "application/pdf",
      "fileSize": 1572864,
      "fileSizeStr": "1.5MB",
      "fileSource": 0,
      "fileSourceName": "申请材料",
      "uploadTime": "2024-06-21 09:15:28",
      "uploadUserName": "李四",
      "fileHash": "c81e728d9d4c2f636f067f89cc14862c"
    }
    // 更多文件记录...
  ],
  "approvalRecordList": [
    {
      "recordId": 3001,
      "nodeName": "部门负责人审批",
      "nodeSort": 1,
```

```
      "dealUserId": 1003,
      "dealUserName": "张三",
      "dealUserDeptName": "市场部",
      "dealType": 0,
      "dealTypeName": "通过",
      "dealRemark": "同意提交法务审核，协议条款需重点核对违约责任部分",
      "dealTime": "2024-06-21 10:30:15",
      "dealIp": "192.168.1.103",
      "dealDevice": "iPhone 14 iOS 16.5"
    },
    {
      "recordId": 3002,
      "nodeName": "法务审核",
      "nodeSort": 2,
      "dealUserId": 1006,
      "dealUserName": "孙七",
      "dealUserDeptName": "法务部",
      "dealType": 1,
      "dealTypeName": "待处理",
      "dealRemark": "",
      "dealTime": "",
```

```
        "dealIp": "",
        "dealDevice": ""
      }
      // 更多审批节点记录...
    ],
    "sealInfo": {
      "sealUserId": "",
      "sealUserName": "",
      "sealTime": "",
      "sealFileList": [] // 已盖章文件列表（状态为“已归档”时返回）
    }
  }
}
```


• 异常响应：

◦ 400：参数错误（如 approvalId 为空或非整数）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无权限查看该申请（如普通用户查看他人申请、审批人查看非本人审批节点的申请）；

◦ 404：指定 approvalId 的申请不存在；

◦ 500：服务器内部错误（如数据库查询异常）。

• 业务逻辑：

1. 验证 Token 有效性，解析当前用户 ID、角色及所属部门；

2. 校验路径参数 approvalId 合法性，查询申请基础信息（审批表）；

3. 权限校验：申请人仅能查看自己发起的申请，审批人仅能查看分配至本人的审批申请，管理员可查看所有申请，未授权用户返回 403 错误；

4. 关联查询补充信息：部门表（部门名称）、用户表（申请人姓名、脱敏手机号）、数据字典表（用章用途名称、紧急程度名称）；

5. 查询该申请关联的所有文件（文件表），筛选状态为“正常”的文件，补充文件大小人性化显示、上传人名称等信息；

6. 查询审批记录明细表，按节点排序（nodeSort）展示所有审批节点记录，已处理节点显示完整处理信息，待处理节点标注“待处理”状态；

7. 若申请状态为“已归档”，查询盖章相关信息（盖章人、盖章时间、已盖章文件列表）；

8. 记录操作日志（操作人 ID、操作类型“查询申请详情”、审批 ID、审批编号）；

9. 组装完整响应数据并返回。

13.2.5.4 撤回用章申请接口：POST /api/v1/approvals/{approvalId}/withdraw

• 功能描述：申请人在申请未通过最终审批（状态为“待审批”“审批中”）时，可撤回申请，撤回后审批流程终止，支持填写撤回原因，便于追溯。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（申请人 Token）

• 路径参数：

◦ approvalId：整数（必填），待撤回申请的唯一 ID。

• 请求体参数：

◦ withdrawReason：字符串（必填），撤回原因（不少于 20 位字符，如“申请材料有误，需补充修改”）。

• 响应数据：


```
{
  "code": 200,
  "message": "申请撤回成功",
  "data": {
    "approvalId": 5001,
    "approvalNo": "2024-DEP01-00001",
    "status": 6,
    "statusName": "已撤回",
```

```
    "withdrawTime": "2024-06-21 11:00:15"
  }
}
```


- 异常响应：

◦ 400：参数错误（如 withdrawReason 长度不足）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户非该申请的申请人，无撤回权限；

◦ 404：指定 approvalId 的申请不存在；

◦ 409：申请状态为“已通过”“已驳回”“已归档”“已撤回”，无法撤回；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性，解析当前用户 ID；

2. 校验路径参数 approvalId 与请求体参数，查询申请信息及申请人 ID;

3. 权限校验：仅申请本人可发起撤回，非申请人返回 403 错误;

4. 状态校验：仅“待审批”“审批中”状态的申请可撤回，其他状态返回 409 错误;

5. 更新审批表状态为“已撤回”，记录撤回原因、撤回时间;

6. 终止当前审批流程，清空未处理节点的审批任务，向相关审批人推送“申请已撤回”通知;

7. 记录操作日志（操作人 ID、操作类型“撤回申请”、审批 ID、审批编号、撤回原因);

8. 返回撤回成功响应。

13.2.5.5 查询待审批列表接口：GET /api/v1/approvals/pending

• 功能描述：审批人查询分配至本人的待处理用章申请列表，支持按申请部门、用章用途、紧急程度筛选，支持分页与排序，便于高效处理审批任务。

• 请求头：

◦ Authorization: Bearer {token}（审批人 Token，需具备“审批用章申请”权限）

• 查询参数：

◦ deptId：整数（可选），按申请所属部门筛选；

◦ purpose：整数（可选），按用章用途筛选；

◦ urgentLevel：整数（可选），按紧急程度筛选（0-普通、1-紧急、2-特急）；

◦ pageNum：整数（必填），页码（默认 1）；

◦ pageSize：整数（必填），每页条数（默认 10，最大 50）；

◦ sortField：字符串（可选），排序字段（如“createTime”“urgentLevel”，默认“urgentLevel desc, createTime desc”）；

◦ sortOrder：字符串（可选），排序方向（仅 sortField 为单个字段时生效）。

• 响应数据：


```
{
  "code": 200,
  "message": "查询成功",
  "data": {
    "total": 8,
    "pageNum": 1,
    "pageSize": 10,
    "list": [
      {
        "approvalId": 5002,
        "approvalNo": "2024-DEP02-00002",
        "title": "XX 产品宣传公文用印申请",
        "deptName": "品牌部",
        "applyUserName": "王五",
```

```
        "applyUserPhone": "139****4567",
        "purposeName": "公文用印",
        "urgentLevel": 1,
        "urgentLevelName": "紧急",
        "submitTime": "2024-06-21 09:30:20",
        "nodeName": "品牌部负责人审批",
        "fileCount": 2
      },
      // 更多待审批记录...
    ]
  }
}
```


- 异常响应：

◦ 400：参数错误（如 pageNum/pageSize 非法）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无审批权限；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与审批人权限，解析当前审批人 ID；

2. 解析查询参数，构建筛选条件（部门、用途、紧急程度）；

3. 关联查询审批表、审批记录明细表，筛选“分配至当前审批人且未处理”的待审批申请；

4. 关联部门表、用户表、数据字典表，补充部门名称、申请人姓名、脱敏手机号、用途名称等信息；

5. 统计每个申请的文件数量，按“紧急程度降序+提交时间降序”默认排序（紧急申请优先展示）；

6. 执行分页查询，返回待审批列表；

7. 记录操作日志（操作人 ID、操作类型“查询待审批列表”、筛选条件）；

8. 返回查询结果。

13.2.5.6 处理审批接口：POST /api/v1/approvals/{approvalId}/deal

• 功能描述：审批人处理分配至本人的待审批申请，支持“通过”“驳回”操作，需填写审批意见，处理后自动流转至下一节点或终止流程，支持业务规则校验。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（审批人 Token，需具备对应审批节点权限）

• 路径参数：

◦ approvalId：整数（必填），待处理申请的唯一 ID。

• 请求体参数：

◦ dealType：整数（必填），处理类型（0-通过、1-驳回）；

◦ dealRemark：字符串（必填），审批意见（不少于 10 位字符，如“同意审批，需确保协议盖章位置规范”）；

◦ nextApproverId：整数（可选），转签审批人 ID（仅 dealType=0 且支持转签时填写）。

• 响应数据：

```
{
  "code": 200,
  "message": "审批处理成功",
  "data": {
    "approvalId": 5002,
    "approvalNo": "2024-DEP02-00002",
    "dealType": 0,
    "dealTypeName": "通过",
    "nextNodeName": "分管领导签批", // 下一审批节点（无则返回“无”）
    "currentStatus": 1,
    "currentStatusName": "审批中"
  }
}
```

• 异常响应：

◦ 400：参数错误（如 dealRemark 长度不足、转签人 ID 不存在）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无该审批节点的处理权限；

◦ 404：指定 approvalId 的申请不存在；

◦ 409：申请状态非“待审批”或“审批中”，或该申请未分配至当前用户；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性，解析当前审批人 ID 与权限；

2. 校验路径参数 approvalId 与请求体参数，查询申请信息、当前审批节点信息；

3. 权限与状态校验：确认申请已分配至当前用户，且状态为“待审批”“审批中”，否则返回 409 错误；

4. 记录审批处理记录：向审批记录明细表插入当前节点处理信息（处理人、处理类型、意见、时间、IP、设备）；

5. 按处理类型执行流程流转：

◦ 若 dealType=0（通过）：查询审批流程的下一节点，若存在下一节点，推送审批任务至对应审批人；若为最后一个节点，更新申请状态为“已通过”，推送“待盖章”通知至盖章端；若填写 nextApproverId，转签至指定审批人，更新节点处理人；

◦ 若 dealType=1（驳回）：按审批流程的驳回规则（驳回至申请人/上一节点），更新申请状态为“已驳回”，推送驳回通知至申请人；

6. 更新审批表的当前状态、处理人 ID、处理时间、驳回意见（仅驳回时）；

7. 记录操作日志（操作人 ID、操作类型“处理审批”、审批 ID、审批编号、处理类型、意见）；

8. 返回处理成功响应及流程流转信息。

13.2.5.7 上传盖章文件接口：POST /api/v1/approvals/{approvalId}/seal-file

• 功能描述：盖章员在申请状态为“已通过”时，上传已盖章的电子文件，文件自动关联对应审批申请，上传完成后申请状态更新为“已归档”，支持文件格式、大小校验及完整性校验。

• 请求头：

◦ Content-Type: multipart/form-data（含文件上传）

◦ Authorization: Bearer {token}（盖章员 Token，需具备“上传盖章文件”权限）

• 路径参数：

◦ approvalId：整数（必填），待上传盖章文件的申请唯一 ID。

• 请求参数（FormData 格式）：

◦ sealFiles：文件数组（必填），已盖章文件（支持 JPG、PNG、PDF 格式，单个文件≤200MB，最多 5 个文件，需与申请材料文件一一对应或覆盖关键页）；

◦ sealRemark：字符串（可选），盖章说明（如“已完成骑缝章加盖，共 3 页”，长度不超过 200 位字符）。

• 响应数据：


```
{
  "code": 200,
  "message": "盖章文件上传成功，申请已归档",
  "data": {
    "approvalId": 5002,
    "approvalNo": "2024-DEP02-00002",
    "status": 5,
    "statusName": "已归档",
    "sealTime": "2024-06-21 15:30:45",
    "sealUserId": 1008,
    "sealUserName": "周八",
    "fileList": [
      {
```

```
        "fileId": 10005,
        "fileName": "XX 产品宣传公文-已盖章.pdf",
        "fileType": "application/pdf",
        "fileSizeStr": "1.8MB",
        "fileHash": "9b3b2692844e0496949f67e5ca88d39a"
      }
      // 更多盖章文件记录...
    ]
  }
}
```


- 异常响应：

◦ 400：参数错误（如文件格式不符、大小超限、文件数量过多）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无上传盖章文件权限；

◦ 404：指定 approvalId 的申请不存在；

◦ 409：申请状态非“已通过”，无法上传盖章文件；

◦ 500：服务器内部错误（如文件存储失败、数据库更新异常）。

• 业务逻辑：

1. 验证 Token 有效性与盖章员权限，解析当前操作人 ID；

2. 校验路径参数 approvalId 合法性，查询申请信息，确认申请状态为“已通过”，否则返回 409 错误；

3. 校验上传文件的格式、大小、数量，不符合要求则返回 400 错误；

4. 上传盖章文件至服务器指定目录，采用“审批编号-盖章-文件名”规则命名，生成文件元数据（名称、路径、哈希值、大小等）；

5. 向文件表插入盖章文件记录，关联当前审批 ID，标记文件来源为“盖章文件”；

6. 更新审批表状态为“已归档”，记录盖章人 ID、盖章时间、盖章说明；

7. 向申请人推送“申请已归档”通知，同步更新申请进度；

8. 记录操作日志（操作人 ID、操作类型“上传盖章文件”、审批 ID、审批编号、文件数量）；

9. 组装响应数据，返回上传成功及申请归档信息。

13.2.5.8 管理员查询审批列表接口：GET /api/v1/approvals/admin

• 功能描述：管理员查询系统所有用章申请列表，支持多维度组合筛选（部门、申请人、状态、时间等），支持分页与排序，便于全局审批监控与统计。

• 请求头：

◦ Authorization: Bearer {token}（管理员 Token，需具备“全局审批查询”权限）

• 查询参数：

◦ approvalNo：字符串（可选），按审批编号精准查询；

◦ deptId：整数（可选），按申请所属部门筛选；

◦ applyUserId：整数（可选），按申请人 ID 筛选；

◦ purpose：整数（可选），按用章用途筛选；

◦ status：整数（可选），按申请状态筛选；

◦ urgentLevel：整数（可选），按紧急程度筛选；

◦ startTime：字符串（可选），申请开始时间（YYYY-MM-DD）；

◦ endTime：字符串（可选），申请结束时间（YYYY-MM-DD）；

◦ keyword：字符串（可选），按申请标题/申请人姓名模糊查询；

◦ pageNum：整数（必填），页码（默认 1）；

◦ pageSize：整数（必填），每页条数（默认 10，最大 100）；

◦ sortField：字符串（可选），排序字段（如“createTime”“approvalNo”）；

◦ sortOrder：字符串（可选），排序方向（asc/desc，默认desc）。

• 响应数据：


```
{
  "code": 200,
  "message": "查询成功",
  "data": {
    "total": 236,
    "pageNum": 1,
    "pageSize": 10,
    "list": [
      {
        "approvalId": 5002,
        "approvalNo": "2024-DEP02-00002",
        "title": "XX产品宣传公文用印申请",
        "deptName": "品牌部",
        "applyUserName": "王五",
```

```
        "purposeName": "公文用印",
        "urgentLevelName": "紧急",
        "status": 5,
        "statusName": "已归档",
        "submitTime": "2024-06-21 09:30:20",
        "approveTime": "2024-06-21 14:10:30",
        "sealTime": "2024-06-21 15:30:45",
        "fileCount": 2,
        "sealUserName": "周八"
      },
      // 更多审批记录...
    ]
  }
}
```


- 异常响应：

◦ 400：参数错误（如日期格式错误、pageNum/pageSize 非法）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无全局审批查询权限；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性与管理员权限；

2. 解析多维度查询参数，构建组合筛选条件；

3. 关联审批表、部门表、用户表、数据字典表，查询符合条件的所有申请数据；

4. 补充审批时间、盖章时间、盖章人姓名等关键信息；

5. 执行分页查询，按指定排序字段与方向排序；

6. 记录操作日志（操作人 ID、操作类型“管理员查询审批列表”、筛选条件）；

7. 返回分页查询结果。

13.2.5.9 导出审批列表接口：GET /api/v1/approvals/export

• 功能描述：管理员导出符合筛选条件的审批列表数据，支持Excel格式，包含申请核心信息、审批流程、归档状态等字段，便于离线统计与存档。

• 请求头：

◦ Authorization: Bearer {token}（管理员Token，需具备“审批导出”权限）

• 查询参数：

◦ 与“管理员查询审批列表接口”筛选参数一致，新增exportFields（可选），指定导出字段（如“approvalNo,title,deptName,statusName,submitTime”）。

• 响应数据：

◦ 响应类型：application/vnd.openxmlformats-officedocument.spreadsheetml.sheet（Excel文件）；

◦ 响应头：Content-Disposition: attachment; filename="审

批列表_20240621.xlsx"。

- 异常响应：

◦ 400：参数错误（如 exportFields 字段不存在）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无审批导出权限；

◦ 500：服务器内部错误（如文件生成失败）。

- 业务逻辑：

1. 验证 Token 有效性与管理员权限；

2. 解析筛选参数与导出字段，查询符合条件的审批数据；

3. 按指定 exportFields 筛选字段，默认导出全部核心字段；

4. 生成 Excel 文件，设置表头、单元格格式，确保数据清晰可读；

5. 触发客户端下载，记录操作日志（操作人 ID、操作类型“导出审批列表”、筛选条件、导出时间）；

6. 大数据量导出时采用异步生成机制，通过系统消息通知管理员下载。

13.2.6 文件管理接口

文件管理接口提供申请材料、盖章文件的查询、下载（V1.0 预留）、替换等功能，确保文件操作的安全性与可追溯性，核心接口如下：

13.2.6.1 查询申请文件列表接口：GET /api/v1/files/approval/{approvalId}

• 功能描述：用户查询指定审批申请关联的所有文件（申请材料+盖章文件），支持按文件来源筛选，获取文件元数据与访问凭证（V1.0 仅返回元数据）。

• 请求头：

◦ Authorization: Bearer {token}（用户 Token，需具备该申请查看权限）

• 路径参数：

◦ approvalId：整数（必填），审批申请唯一 ID。

• 查询参数：

◦ fileSource：整数（可选），按文件来源筛选（0-申请材料、1-盖章文件）。

• 响应数据：


```
{
  "code": 200,
  "message": "查询成功",
  "data": [
    {
      "fileId": 10002,
      "fileName": "补充协议.pdf",
      "fileType": "application/pdf",
      "fileSizeStr": "1.5MB",
```

```
    "fileSource": 0,
    "fileSourceName": "申请材料",
    "uploadTime": "2024-06-21 09:15:28",
    "uploadUserName": "李四",
    "fileHash": "c81e728d9d4c2f636f067f89cc14862c",
    "fileStatus": 0,
    "fileStatusName": "正常"
  },
  {
    "fileId": 10005,
    "fileName": "XX产品宣传公文-已盖章.pdf",
    "fileType": "application/pdf",
    "fileSizeStr": "1.8MB",
    "fileSource": 1,
    "fileSourceName": "盖章文件",
    "uploadTime": "2024-06-21 15:30:45",
    "uploadUserName": "周八",
    "fileHash": "9b3b2692844e0496949f67e5ca88d39a",
    "fileStatus": 0,
    "fileStatusName": "正常"
  }
]
```

}

- 异常响应：

◦ 400：参数错误（如 approvalId 为空或非整数）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无该申请文件查看权限；

◦ 404：指定 approvalId 的申请或文件不存在；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性，解析用户 ID 与角色；

2. 校验路径参数 approvalId 与查询参数，查询申请信息并验证用户查看权限；

3. 按审批 ID+文件来源筛选文件表，获取符合条件的文件元数据；

4. 补充文件大小人性化显示、上传人名称、文件状态等信息；

5. 记录操作日志（操作人 ID、操作类型“查询申请文件”、审批 ID、文件来源）；

6. 返回文件列表数据。

13.2.6.2 替换申请材料文件接口：POST /api/v1/files/{fileId}/replace

• 功能描述：申请人在申请状态为“已驳回”时，可替换原申请材料文件，替换后原文件标记为“已替换”，保留历史记录，新文件生成新文件 ID 并关联原审批。

• 请求头：

◦ Content-Type: multipart/form-data（含文件上传）

◦ Authorization: Bearer {token}（申请人 Token）

• 路径参数：

◦ fileId：整数（必填），待替换的原文件唯一 ID。

• 请求参数（FormData 格式）：

◦ newFile：文件（必填），新的申请材料文件（格式、大小需符合系统要求，与原文件类型一致）；

◦ replaceReason：字符串（必填），替换原因（不少于 10 位字符，如“补充最新版本协议，修正条款错误”）。

• 响应数据：


```
{
  "code": 200,
  "message": "文件替换成功",
  "data": {
    "oldFileId": 10002,
    "oldFileName": "补充协议.pdf",
    "newFileId": 10006,
    "newFileName": "补充协议-V2.pdf",
    "replaceTime": "2024-06-21 16:00:30",
    "approvalId": 5001,
```

"approvalNo": "2024-DEP01-00001"
}
}

• 异常响应：

◦ 400：参数错误（如文件格式/大小不符、replaceReason 长度不足）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户非原文件上传人，无替换权限；

◦ 404：指定 fileId 的文件不存在；

◦ 409：申请状态非“已驳回”，或原文件类型非“申请材料”，无法替换；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性，解析申请人 ID；

2. 校验路径参数 fileId 与上传文件，查询原文件信息及关联审批信息；

3. 权限与状态校验：仅原文件上传人可替换，且关联申请状态为“已驳回”，否则返回 403/409 错误；

4. 校验新文件格式、大小与原文件一致，不符合则返回 400 错误；

5. 上传新文件至服务器，生成新文件元数据，插入文件表并关联原审批 ID；

6. 更新原文件状态为“已替换”，记录替换文件 ID；

7. 记录操作日志（操作人 ID、操作类型“替换申请文件”、原文件 ID、新文件 ID、替换原因）；

8. 返回文件替换成功响应。

13.2.7 日志管理接口

日志管理接口面向管理员，提供登录日志、操作日志、安全日志的查询、筛选、导出功能，支持审计追溯与安全排查，核心接口如下：

13.2.7.1 查询登录日志接口：GET /api/v1/logs/login

• 功能描述：管理员查询系统所有用户的登录日志，支持多维度筛选与分页排序，全面追溯账号登录轨迹，为账号安全审计与异常排查提供依据。

• 请求头：

◦ Authorization: Bearer {token}（管理员 Token，需具备“日志查询”权限）

• 查询参数：

◦ username：字符串（可选），按用户名模糊查询（如“zhangsan”“li”）；

◦ loginIp：字符串（可选），按登录 IP 精准查询（支持 IPv4/IPv6 格式，如“192.168.1.100”）；

◦ loginResult：整数（可选），按登录结果筛选（0-失败、1-成功）；

◦ loginLocation：字符串（可选），按登录地点模糊查询（如“北京市”）；

◦ startTime：字符串（可选），登录开始时间（精确到秒，格式“YYYY-MM-DD HH:mm:ss”）；

◦ endTime：字符串（可选），登录结束时间（格式“YYYY-MM-DD HH:mm:ss”）；

◦ pageNum：整数（必填），页码（默认 1）；

◦ pageSize：整数（必填），每页条数（默认 10，最大 50）；

◦ sortField：字符串（可选），排序字段（如“loginTime”“username”）；

◦ sortOrder：字符串（可选），排序方向（asc-升序、desc-降序，默认“loginTime desc”）。

- 响应数据：


```
{
  "code": 200,
  "message": "查询成功",
  "data": {
    "total": 1568,
    "pageNum": 1,
    "pageSize": 10,
    "list": [
      {
        "logId": 8921,
        "username": "zhangsan",
        "userNickname": "张三",
        "loginIp": "192.168.1.100",
        "loginDevice": "Windows 11 Chrome 120.0",
        "loginLocation": "北京市朝阳区",
        "loginResult": 1,
        "loginResultName": "成功",
        "failReason": "",
        "loginTime": "2024-06-21 09:30:15",
        "sessionId":
```

```
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...",
        "logoutTime": "2024-06-21 18:05:22"
      },
      {
        "logId": 8920,
        "username": "lisi",
        "userNickname": "李四",
        "loginIp": "192.168.1.101",
        "loginDevice": "iPhone 14 iOS 16.5",
        "loginLocation": "上海市浦东新区",
        "loginResult": 0,
        "loginResultName": "失败",
        "failReason": "密码错误",
        "loginTime": "2024-06-21 09:25:33",
        "sessionId": "",
        "logoutTime": ""
      }
      // 更多登录日志记录...
    ]
  }
}
```


- 异常响应：

◦ 400：参数错误（如日期格式错误、pageNum/pageSize 非法）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无日志查询权限；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性与管理员权限；

2. 解析多维度查询参数，构建组合筛选条件（支持用户名模糊匹配、IP 精准匹配、时间范围筛选等）；

3. 执行分页查询，关联用户表获取用户昵称，补充登录结果名称（成功/失败）；

4. 按指定排序字段与方向排序（默认按登录时间倒序，最新记录优先展示）；

5. 记录操作日志（操作人 ID、操作类型“查询登录日志”、筛选条件）；

6. 返回分页查询结果。

13.2.7.2 查询操作日志接口：GET /api/v1/logs/operate

• 功能描述：管理员查询系统所有用户的业务操作日志，支持按操作人、部门、模块、操作类型筛选，全面追溯业务操作轨迹，为审计与问题排查提供支撑。

• 请求头：

◦ Authorization: Bearer {token}（管理员 Token，需具备“日志查询”权限）

• 查询参数：

◦ operateUserId：整数（可选），按操作人 ID 筛选；

◦ deptId：整数（可选），按操作人所属部门筛选；

◦ operateModule：字符串（可选），按操作模块筛选（如“用章申请”“审批管理”“账号管理”）；

◦ operateType：字符串（可选），按操作类型筛选（如“提交”“审批”“创建”“修改”）；

◦ operateResult：整数（可选），按操作结果筛选（0-失败、1-成功）；

◦ startTime：字符串（可选），操作开始时间（YYYY-MM-DD HH:mm:ss）；

◦ endTime：字符串（可选），操作结束时间（YYYY-MM-DD HH:mm:ss）；

◦ keyword：字符串（可选），按操作对象、操作内容模糊查询；

◦ pageNum：整数（必填），页码（默认 1）；

◦ pageSize：整数（必填），每页条数（默认 10，最大 50）；

◦ sortField：字符串（可选），排序字段（如“operateTime”）；

◦ sortOrder：字符串（可选），排序方向（默认“operateTime desc”）。

• 响应数据：


```
{
  "code": 200,
  "message": "查询成功",
  "data": {
    "total": 3286,
    "pageNum": 1,
    "pageSize": 10,
    "list": [
      {
        "logId": 15632,
        "operateUserId": 1002,
        "operateUserName": "李四",
        "deptId": 201,
        "deptName": "市场部",
        "operateModule": "用章申请",
```

```
        "operateType": "提交",
        "operateObject": "审批单（编号：2024-DEP01-00001）",
        "operateIp": "192.168.1.102",
        "operateDevice": "Windows 11 Chrome 120.0",
        "operateResult": 1,
        "operateResultName": "成功",
        "operateContent": "提交用章申请，标题：XX 项目合作协议盖章申请，用章用途：合同签署",
        "errorMsg": "",
        "operateTime": "2024-06-21 09:15:30"
      },
      {
        "logId": 15631,
        "operateUserId": 1003,
        "operateUserName": "张三",
        "deptId": 201,
        "deptName": "市场部",
        "operateModule": "审批管理",
        "operateType": "审批",
        "operateObject": "审批单（编号：2024-DEP01-00001）",
```

```
        "operateIp": "192.168.1.103",
        "operateDevice": "iPhone 14 iOS 16.5",
        "operateResult": 1,
        "operateResultName": "成功",
        "operateContent": "审批通过编号为 2024-DEP01-00001 的申请，审批意见：同意提交法务审核",
        "errorMsg": "",
        "operateTime": "2024-06-21 10:30:15"
      }
      // 更多操作日志记录...
    ]
  }
}
```


- 异常响应：

◦ 400：参数错误（如日期格式错误、操作模块/类型非法）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无日志查询权限；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性与管理员权限；

2. 解析查询参数，构建组合筛选条件（支持多维度精准筛选与关键词模糊匹配）；

3. 关联用户表、部门表获取操作人姓名、部门名称；

4. 执行分页查询，按默认操作时间倒序排序；

5. 记录操作日志（操作人 ID、操作类型“查询操作日志”、筛选条件）；

6. 返回分页查询结果。

13.2.7.3 导出日志接口：GET /api/v1/logs/export

• 功能描述：管理员导出符合筛选条件的登录日志或操作日志，支持 Excel 格式，包含日志核心字段，便于离线审计存档与长期追溯。

• 请求头：

◦ Authorization: Bearer {token}（管理员 Token，需具备“日志导出”权限）

• 查询参数：

◦ logType：字符串（必填），日志类型（login-登录日志、operate-操作日志）；

◦ 其他筛选参数：与对应日志查询接口的筛选参数一致，新增 exportFields（可选），指定导出字段（如“username,loginTime,loginIp,loginResultName”）。

• 响应数据：

◦ 响应类型：application/vnd.openxmlformats-officedocument.spreadsheetml.sheet（Excel 文件）；

◦ 响应头：Content-Disposition: attachment; filename="登录日志_20240621.xlsx"（或“操作日志_20240621.xlsx”）。

• 异常响应：

◦ 400：参数错误（如 logType 非法、exportFields 字段不存在）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无日志导出权限；

◦ 500：服务器内部错误（如文件生成失败）。

• 业务逻辑：

1. 验证 Token 有效性与管理员权限；

2. 解析日志类型与筛选参数，按 logType 查询对应日志数据；

3. 按指定 exportFields 筛选导出字段，默认导出全部核心字段；

4. 生成 Excel 文件，按日志类型设置表头与数据格式，确保信

息清晰可读；

5. 触发客户端下载，记录操作日志（操作人 ID、操作类型“导出日志”、日志类型、筛选条件、导出时间）；

6. 大数据量导出（如超过 1000 条）时采用异步生成机制，通过系统消息通知管理员下载。

13.2.8 系统配置接口

系统配置接口面向管理员，提供全局参数配置、审批流程配置、数据字典维护等功能，支持系统动态适配业务需求，无需修改代码，核心接口如下：

13.2.8.1 查询系统配置接口：GET /api/v1/configs

• 功能描述：管理员查询系统所有全局配置参数，支持按配置类型筛选，获取配置键、配置值及说明，为配置调整提供参考。

• 请求头：

◦ Authorization: Bearer {token}（管理员 Token，需具备

“系统配置查询”权限）

• 查询参数：

◦ configType：字符串（可选），按配置类型筛选（如“安全配置”“业务配置”“存储配置”）。

• 响应数据：


```
{
  "code": 200,
  "message": "查询成功",
  "data": [
    {
      "configId": 1,
      "configKey": "password_strength",
      "configValue": "12 位（含大小写字母+数字+特殊符号）
",
      "configName": "密码复杂度要求",
      "configType": "安全配置",
      "remark": "适用于新注册账号及密码修改",
      "sort": 10,
      "createTime": "2024-05-01 10:00:00",
```

```
      "updateTime": "2024-05-01 10:00:00"
    },
    {
      "configId": 5,
      "configKey": "file_upload_max_size",
      "configValue": "209715200",
      "configName": "单个文件上传最大限制",
      "configType": "存储配置",
      "remark": "单位：字节（200MB）",
      "sort": 20,
      "createTime": "2024-05-01 10:00:00",
      "updateTime": "2024-06-10 14:20:30"
    }
    // 更多配置参数...
  ]
}
```


- 异常响应：

  - 401：Token 无效、已过期或未携带 Token；

  - 403：当前用户无系统配置查询权限；

◦ 500：服务器内部错误。

• 业务逻辑：

1. 验证 Token 有效性与管理员权限；

2. 解析查询参数，按配置类型筛选系统配置表数据；

3. 按排序字段排序后返回配置列表；

4. 记录操作日志（操作人 ID、操作类型“查询系统配置”、筛选类型）；

5. 返回查询结果。

13.2.8.2 更新系统配置接口：PUT /api/v1/configs/{configId}

• 功能描述：管理员修改指定全局配置参数的配置值，修改后即时生效，支持配置值格式校验，确保配置合规。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理员 Token，需具备“系统配置修改”权限）

• 路径参数：

◦ configId：整数（必填），配置参数唯一 ID。

• 请求体参数：

◦ configValue：字符串（必填），新配置值（需符合该配置的格式要求，如数值型配置需为整数）；

◦ remark：字符串（可选），新备注信息（更新配置说明）。

• 响应数据：


```
{
  "code": 200,
  "message": "配置更新成功",
  "data": {
```

```
    "configId": 5,
    "configKey": "file_upload_max_size",
    "configValue": "314572800",
    "configName": "单个文件上传最大限制",
    "updateTime": "2024-06-21 16:30:45",
    "updateByName": "系统管理员"
  }
}
```


- 异常响应：

◦ 400：参数错误（如配置值格式不符合要求，如将非数值填入大小限制配置）；

◦ 401：Token 无效、已过期或未携带 Token；

◦ 403：当前用户无系统配置修改权限；

◦ 404：指定 configId 的配置不存在；

◦ 500：服务器内部错误。

- 业务逻辑：

1. 验证 Token 有效性与管理员权限，解析操作人 ID；

2. 校验路径参数 configId 与请求体参数，查询配置当前信息；

3. 按配置键（configKey）对应的规则校验新配置值格式（如密码复杂度配置需符合规则描述、数值型配置需为有效整数）；

4. 更新系统配置表中对应记录的配置值、备注、修改人 ID、修改时间；

5. 记录操作日志（操作人 ID、操作类型“更新系统配置”、配置 ID、配置键、修改前后值）；

6. 返回配置更新成功响应。

13.2.8.3 配置审批流程接口：POST /api/v1/approval-flows

• 功能描述：管理员创建或编辑审批流程，设置流程名称、适配用章用途、驳回规则及节点配置，支持灵活定制差异化审批流程。

• 请求头：

◦ Content-Type: application/json

◦ Authorization: Bearer {token}（管理员 Token，需具备“审批流程配置”权限）

• 请求体参数：

◦ flowId：整数（可选），流程 ID（新增流程不传，编辑流程必填）；

◦ flowName：字符串（必填），流程名称（如“合同签署审批流程”）；

◦ purposeType：整数（必填），适配用章用途（关联数据字典表，如 0-合同签署）；

◦ status：整数（可选），流程状态（0-禁用、1-启用，默认 1）；

◦ rejectRule：整数（必填），驳回规则（0-驳回至申请人、1-

驳回至上一节点);

◦ urgentTimeout：整数（可选），紧急审批时效（单位小时，如24);

◦ nodes：数组（必填），审批节点列表，含 nodeName（节点名称）、nodeSort（排序）、approverType（审批人类型）、relatedId（关联 ID）等;

◦ remark：字符串（可选），流程备注。

• 响应数据：

```
{
  "code": 200,
  "message": "审批流程配置成功",
  "data": {
    "flowId": 3,
    "flowName": "合同签署审批流程",
    "purposeTypeName": "合同签署",
    "status": 1
  }
}
```

• 异常响应：核心含 400 参数错误、401 Token 失效、403 权限不足、409 流程名称重复等。

• 业务逻辑：校验参数合法性，新增/更新流程主表与节点表，关联用章用途，记录操作日志并返回结果。

13.2.8.4 维护数据字典接口：POST /api/v1/dicts

• 功能描述：管理员新增或编辑数据字典项（如用章用途、紧急程度），支持字典类型分类维护，统一系统枚举数据标准。

• 请求头：同系统配置接口

• 请求体参数：含 dictType（字典类型）、dictCode（编码）、dictValue（显示值）、status（状态）等。

• 响应数据：返回字典 ID、类型、编码及操作结果。

• 业务逻辑：校验编码唯一性，新增/更新字典表，记录日志。

13.3 接口安全补充说明

• 接口限流：核心接口（登录、提交申请）设限流策略，单 IP 单日请求不超过 1000 次，避免恶意请求攻击；

• 数据脱敏：所有响应中手机号、身份证号等敏感信息均脱敏展示，仅授权接口可获取完整数据；

• 签名验证（可选）：第三方系统集成时，支持接口请求签名验证，通过 AppKey+时间戳+签名机制保障接口调用安全。

十四、风险与应对措施

14.1 项目风险

• 需求变更风险：需求频繁变更导致工期延误，应对：建立需求变更审批流程，明确变更范围与影响，同步调整进度计划；

• 技术适配风险：部署环境与系统不兼容，应对：提前开展环境调研与适配测试，提供多环境部署方案；

• 数据迁移风险（若有）：历史数据迁移丢失或错乱，应对：迁移前全量备份，分批次迁移并校验数据一致性；

• 用户接受度风险：用户不熟悉系统操作，应对：优化操作界面，开展多层级培训，提供线上辅导。

14.2 运行风险

• 系统性能风险：高并发下响应缓慢，应对：优化数据库索引与SQL，配置负载均衡，定期性能巡检；

• 数据安全风险：数据泄露或篡改，应对：强化加密存储与访问控制，定期安全扫描，完善日志审计；

• 故障风险：服务器宕机或服务中断，应对：部署主备架构，建立故障应急预案，提供7×24小时故障响应。

十五、结语

15.1 产品价值总结

本软件聚焦企业用章管理核心痛点，通过线上申请、智能审批、全程追溯、安全存储等一体化功能，构建了高效、合规、可追溯的用章管理体系。产品以模块化设计适配不同规模企业需求，兼顾操作便捷性与数据安全性，有效解决传统用章流程繁琐、效率

低下、风险难控等问题，为企业数字化办公转型提供核心支撑。

15.2 技术与服务承诺

产品严格遵循行业技术标准与数据安全规范，保障系统稳定运行与用户数据隐私。后续将持续基于用户反馈与业务发展需求，迭代优化功能模块、提升系统性能，提供及时的技术支持与升级服务，确保产品始终贴合企业实际应用场景。

15.3 适用范围与展望

本软件适用于各类需要规范用章管理的企业及组织，涵盖合同签署、公文流转、业务审批等多场景使用需求。未来将进一步拓展功能边界，探索与企业 OA、CRM 等系统的深度集成，打造更全面的办公协作生态，为用户创造更大价值。