

十一、服务方案及承诺

11.1 售后服务方案具体内容

11.1.1 服务定义

本方案基于濮阳市政府网站集约化建设运维项目需求，以“专业高效、安全可靠、用户至上”为核心原则，明确项目全生命周期的服务内容、标准与承诺，确保项目从建设到运维的每一环均满足政务服务数字化、规范化要求，助力濮阳市打造高效、安全、便民的政府网站集约化平台。

11.1.2 服务目标

稳定性目标：确保集约化平台年可用性，核心业务模块（如政务公开信息发布、依申请公开处理、互动交流审核）无故障运行，页面加载，数据查询响应。

安全性目标：建立全流程安全防护体系，有效拦截 XSS 攻击、SQL 注入等恶意行为，实现平台零重大安全事故，数据泄露事件发生率为 0，及时修复发现的安全漏洞。

响应效率目标：建立分级响应机制，确保一般问题 15 分钟内响应、复杂问题 2 小时内解决、重大问题 4 小时内恢复基本功能。

业务适配目标：根据濮阳市政府办及相关部门业务需求变化（如基层政务公开扩展领域建设、监管功能升级），及时优化平台功能，保障政务服务高效开展。

11.1.3 服务范围

平台覆盖范围：包括濮阳市人民政府门户网站、集约化平台内所有部门网站、政务公开平台、基层政务公开标准化规范化监管平台，以及“网上依申请公开提交功能”等专项功能模块。

服务内容范围：涵盖平台日常运维、技术支持、安全防护、数据保障、功能维护与升级、SSL 证书管理、管理员培训与咨询等，具体对应政府网站技术运维及运行保障服务 13 项工作内容。

服务对象范围：

直接对象：濮阳市人民政府办公室项目对接部门及负责人。

间接对象：集约化平台内各部门网站管理员、基层政务公开平台管理员、政务公开信息发布人员、互动交流审核人员等。

针对本项目平台的全生命周期运行需求，提供以下专属服务内容：

1. 日常技术支持：通过热线、在线客服、邮件等渠道，解答用户在平台操作、功能使用中的疑问，协助处理账号管理、权限配置等基础问题。

2. 定期维护服务：每月进行 1 次远程系统健康检查，包括软件版本兼容性、数据库冗余清理、日志异常分析；每季度安排 1 次上门维护，检查服务器硬件运行状态、网络链路稳定性，提供针对性优化建议。

3. 功能适配支持：根据用户业务调整需求，提供小范围功能参数配置修改（如报表模板调整、流程节点优化），确保平台与业务场景同步适配。

4. 服务跟踪与复盘：建立“一问题一档案”机制，详细记录问题描述、处理过程、解决结果及用户反馈，每月生成《售后服务总结报告》，同步用户方负责人。



11.1.4 项目建设阶段服务

1. 需求深化与方案优化

- 组建专项需求调研小组，在项目启动后 7 个工作日内，完成与濮阳市人民政府办公室及各区县、部门的需求对接，形成《需求深化报告》，并根据反馈优化技术方案，确保方案贴合实际政务场景。

- 针对集约化平台（网站群管理系统、内容管理系统等）的功能模块，提供 3 轮方案评审服务，邀请甲方及行业专家参与，确保建设内容符合国家《政府网站集约化试点工作方案》及河南省相关要求。

2. 平台开发与部署服务

- 按项目实施方案进度，完成云基础环境搭建、系统开发、数据迁移等工作，每阶段结束后提交《阶段成果报告》，含功能清单、测试报告等资料，接受甲方阶段性验收。
- 提供“一对一”技术对接服务，为甲方指定的技术对接人提供实时响应，解决开发过程中的需求调整、技术疑问。

3. 系统测试与联调服务

- 组织专业测试团队，开展功能测试、性能测试、安全测试、兼容性测试，对测试发现的问题 100% 整改闭环，整改后重新测试直至通过。
- 协助甲方完成与各部门现有业务系统（如政务服务平台、数据共享平台）的联调，确保数据互联互通，联调期间安排专人驻场支持，直至系统协同运行正常。

4. 上线迁移与过渡服务

- 制定详细的网站迁移方案，明确迁移步骤、时间节点及风险应对措施，迁移前对原有网站数据进行 3 次全量备份，确保数据无丢失。
- 提供“试点迁移+全面推广”服务，先选择 2-3 个部门网站完成试点迁移，总结经验后再推广至全市，迁移期间保障原有网站正常运行，实现“无缝过渡”。

11. 1. 5 项目运维阶段服务

5. 基础设施运维服务

- 对云服务器、存储设备、网络设备等基础设施进行 7×24 小时监控，监控指标包括 CPU 使用率、内存占用、网络带宽、存储容量等，15 分钟内发出预警，30 分钟内启动优化。
- 每月开展 1 次基础设施巡检，包含设备运行状态、潜在风险及优化建议；每季度进行 1 次设备性能优化，确保基础设施支撑能力满足平台运行需求。

6. 平台系统运维服务

- 对网站群管理系统、内容管理系统、智能搜索平台等核心系统，提供 7×24 小时故障响应，一般故障（如单个栏目无法访问）2 小时内解决，重大故障 30 分钟内响应、4 小时内恢复。
- 按季度提供系统升级服务，包含功能优化、漏洞修复、兼容性提升等，升级前提交《升级方案》，明确升级内容、时间（避开业务高峰，如夜间或周末）及回滚预案，升级后提供《升级验收报告》。

7. 数据运维服务

- 对统一信息资源库进行日常维护，包括数据更新、清洗、备份，每日进行增量备份，每周进行全量备份，备份数据异地存储，确保数据丢失时可在 1 小时内恢复。
- 每月开展 1 次数据质量检查，针对数据重复、错误、缺失等问题进行整改，形成《数据质量报告》；协助各部门完成数据归集，提供数据接口对接指导，确保归集数据符合标准。

8. 安全运维服务

- 提供 7×24 小时安全监测，通过安全防护平台实时识别网络攻击、页面篡改、敏感信息泄露等风险，发现异常后 10 分钟内预警，30 分钟内启动处置流程。

- 每月开展 1 次安全漏洞扫描，每季度进行 1 次渗透测试，每年开展 1 次安全应急演练，形成《安全报告》及《演练总结》；协助甲方应对网络安全事件，配合完成上级部门的安全检查。

9. 用户支持服务

- 建立用户支持体系：（7×24 小时）、在线客服（工作日 8:30-17:30），安排专人驻场，解答各部门工作人员的操作疑问。
- 每月收集 1 次用户反馈，针对高频问题更新，并通过培训、现场指导等方式，帮助用户提升平台使用能力。

11.1.6 专项增值服务

10. 定制化需求响应

- 项目建设及运维期间，针对甲方提出的合理定制化需求（如新增特色服务栏目、优化搜索算法），在 5 个工作日内明确实现路径、时间及成本，经甲方确认后推进实施。

11. 培训与知识转移

- 除项目培训方案中的集中培训外，每年提供 2 次免费专项培训（如新版功能使用、安全防护进阶），培训内容根据甲方需求定制，确保相关人员持续掌握平台操作技能。
- 向甲方技术团队提供系统技术文档（如架构图、接口手册、源码注释），协助甲方掌握平台核心技术，降低后期运维依赖。

11.2 解决问题的响应时间及措施

11.2.1 响应时间标准

- (1) 特级故障（平台整体瘫痪、数据传输中断）：15 分钟内响应，技术团队立即启动应急流

程，1 小时内提供临时替代方案，4 小时内完成修复。

(2) 一级故障（核心功能失效、批量用户操作异常）：15 分钟内响应，1 小时内明确故障原因，2 小时内解决。

(3) 二级故障（单一功能异常、少量用户受影响）：15 分钟内响应，1 小时内解决。

(4) 咨询类问题（操作指导、功能说明）：15 分钟内响应，30 分钟内提供清晰解答。

11.2.2 处理措施

(1) 7×24 小时服务通道（热线电话 18790962228），确保问题全天候接收，客服专员 10 分钟内完成问题分级登记。

(2) 建立“故障处理绿色通道”，特级/一级故障直接升级至技术总监督办，协调 3 人以上技术小组集中攻坚；处理过程每 2 小时向用户同步进度，避免信息断层。

(3) 对于需跨部门协作的问题，服务主管牵头成立临时专项组，明确各方权责与时间节点，确保高效推进。

（一）团队保障

1. 组建“专项服务团队”，含项目经理 1 名（5 年以上政府网站项目经验）、技术负责人 1 名（10 年以上系统架构经验）、运维工程师 3 名（具备云计算、安全认证）、驻场人员 1 名（熟悉政务业务），团队成员全程投入项目，不兼任其他项目核心角色。
2. 建立“备份人员机制”，每个核心岗位配备 1 名备份人员，确保原岗位人员休假、离职时，备份人员能立即接手工作，保障服务不中断。

（二）技术保障

3. 搭建“服务支撑平台”，整合故障上报、工单管理、监控预警功能，实现服务全流程可视化，甲方可通过平台实时查看服务进度、故障处理状态。

4. 建立“技术储备库”，储备政府网站集约化相关的技术方案、安全漏洞库、应急处置预案，确保能快速应对各类技术问题；与云服务商、安全厂商建立合作，获取技术支持优先级。

（三）制度保障

5. 制定《服务管理制度》《故障处理规范》《安全运维手册》等制度文件，明确服务流程、责任分工、考核标准，确保服务标准化。
6. 建立“服务考核机制”，每月对服务团队进行考核（指标含响应及时率、故障解决率、用户满意度），考核结果与绩效挂钩，激励团队提升服务质量。

（四）应急保障

7. 制定《重大故障应急预案》《网络安全事件应急预案》，明确应急组织架构、处置流程、责任人员，每年开展2次应急演练，确保应急响应高效。
8. 储备应急资源，包括备用服务器、应急网络设备、离线备份数据，确保发生重大故障时，能快速启动备用资源，降低业务影响。

11.2.3 问题分类标准

根据问题影响范围、紧急程度及处理难度，将平台问题划分为三级，具体分类如下：

问题级别	定义	典型案例	处理优先级
一级（一般问题）	影响范围小，仅涉及单个用户或单个非核心功能，不影响平台整体运行，处理难度低	1. 管理员操作疑问（如模板管理字段设置）；2. 单个栏目静态化发布失败；3. 投票问卷参数配置错误	低，按常规流程处理
二级（较复杂问题）	影响范围较大，涉及多个用户或单个核心功能，可能导致部分业务中断，处理难度	1. 某部门网站域名解析异常，无法访问；2. 内容管理模块联合查询功能故障；3.	中，优先调配资源处理

	中等	智能统计系统数据统计不准确	
三级（重大问题）	影响范围广，涉及全平台或多个核心功能，导致平台整体瘫痪或重大业务中断，处理难度高	1. 平台遭受大规模 DDoS 攻击，无法访问；2. 数据库损坏，数据丢失；3. 多个部门网站同时出现网页篡改	高，立即启动应急响应

（一）问题上报渠道

为确保政府工作人员能快速反馈问题，我方提供 4 种上报渠道，覆盖不同场景需求：

7×24 小时售后服务热线

热线号码：18790962228（提前向濮阳市政府办及各部门公布）。

人员接听后，1 分钟内了解问题核心（级别、影响范围、现象描述），并在《售后服务问题台账》中记录；若可即时解答（如一般操作问题），30 分钟内提供解决方案；若无法即时解答，明确告知用户“问题已转至对应专员，1 小时内反馈处理进度”。

售后服务专属邮箱

邮箱地址：[2836483563@qq.com 售后专属邮箱]，由业务咨询专员每日 8:00-20:00 值守，2 小时内回复所有邮件。



邮件要求：用户在邮件主题中注明“问题级别+部门+问题简述”（如“二级问题-市住建局-域名 SSL 证书报错”），正文需详细描述问题现象、操作步骤、截图（如有），便于快速定位。

处理流程：专员接收邮件后，分类登记至台账，转对应工程师处理，处理完成后通过邮件反馈解决方案及结果，用户确认后闭环。

平台内置在线客服

部署位置：集约化平台管理后台右上角“售后咨询”入口，支持 PC 端与移动端适配。

服务时间：工作日 8:30-17:30（覆盖政府工作时间），实时在线，响应时间 30 秒。

功能支持：

文字咨询：直接解答一般操作问题；

远程协助：若用户同意，可通过内置远程工具协助操作，解决配置类问题；

问题工单：若问题复杂，可在线生成工单，自动同步至《售后服务问题台账》，并告知用户工单编号（用于查询进度）。

紧急问题现场支持申请

适用场景：三级重大问题（如平台瘫痪、数据丢失），或通过远程无法解决的复杂问题。

申请流程：用户通过热线或邮箱提交《现场支持申请单》，注明问题描述、影响范围、紧急程度，售后服务总负责人 15 分钟内审批，审批通过后立即安排技术团队前往濮阳市政府办指定地点现场处理，市区内 1 小时内到达，县域内 2 小时内到达。

11.2.4 分级响应时间承诺

针对不同级别的问题，我方严格遵守以下响应时限，确保问题高效解决：

问题级别	响应时限（从问题上报到首次反馈）	解决时限（从问题确认到彻底解决）	进度反馈频率
一级（一般问题）	30 分钟内（热线即时响应，邮箱 2 小时内响应）	最长 2 个工作日	每日反馈 1 次（若 24 小时内未解决）
二级（较复杂问题）	1 小时内（无论何种上报渠道）	最长 3 个工作日（需外部协作的，最长 5 个工作日）	每 6 小时反馈 1 次
三级（重大问题）	15 分钟内（售后总负责人亲自响应）	4 小时内恢复基本功能，24 小时内彻底解决	每 30 分钟反馈 1 次（直至基本功能恢复）

11.2.5 问题处理流程

建立“上报-登记-分派-处理-验证-闭环-复盘”的全流程问题处理机制，确保每个环节可追溯、可管控：

问题上报与登记：用户通过任一渠道上报问题后，专员在《售后服务问题台账》中记录关键信息，包括：问题编号（自动生成，格式：SY+年月日+序号）、上报时间、上报人、部门、联系方式、问题级别、问题描述。

问题分派：

一级问题：由业务咨询专员或运维专员直接处理；

二级问题：技术支持组长/业务咨询组长分派给对应工程师；

三级问题：售后服务总负责人立即组织技术支持工程师、数据库工程师等成立临时处理小组，牵头处理。

问题处理：

工程师接到任务后，先通过远程排查（如查看系统日志、性能监控数据）或与用户沟通，定位问题原因；

制定处理方案（重大问题需提交《紧急问题处理方案》给濮阳市政府办确认），实施方案并记录处理过程（如修改的配置、执行的命令）；

若需外部协作（如服务器厂商、云存储服务商），由技术支持组长负责对接，每 2 小时向用户同步协作进度。

问题验证：

处理完成后，工程师先自行验证（如测试功能是否恢复、数据是否完整）；

再通知用户进行验证，用户确认问题解决后，在《问题处理确认单》上签字或盖章；

若用户反馈未解决，工程师需重新排查，直至问题闭环。



复盘总结：

每周对已处理问题进行汇总分析，统计问题类型（如功能故障、操作失误、安全问题）、高发模块，形成《周问题分析报告》；

对三级重大问题，处理完成后 3 个工作日内组织复盘会议，分析问题原因、处理过程中的不足，制定改进措施（如优化应急预案、加强培训），形成《重大问题复盘报告》提交濮阳市政府办。

11.3 售后服务人员配置及岗位分工

11.3.1 团队架构设计

我方将组建专属“濮阳市政府网站集约化项目售后服务团队”，采用“总负责人+专项小组”的架构模式，确保服务专业、高效，具体架构如下：

序号	岗位设置	人数	直接汇报对象	核心服务领域
1	售后服务总负责人	1 名	濮阳市政府办项目负责人、我方公司项目总监	统筹服务全局，协调重大问题
2	技术支持组长	1 名	售后服务总负责人	牵头技术问题解决，管理技术工程师
3	技术支持工程师	3 名	技术支持组长	平台故障排查、性能优化、安全防护
4	业务咨询组长	1 名	售后服务总负责人	牵头业务问题解答，管理咨询专员
5	业务咨询专员	2 名	业务咨询组长	政务公开、依申请公开等业务指导
6	运维专员	2 名	技术支持组长	日常巡检、数据备份、日志监控

11.3.2 售后服务人员配置及岗位分工

(1)售后服务总负责人（1名）：5年以上同行业售后服务管理经验，负责对接用户方项目负责人，制定服务计划，审核服务报告，处理服务争议，每月组织内部服务质量复盘。

(2)技术负责人（3名）：具备4年以上平台运维经验，熟悉本项目服务器架构与数据库技术，负责故障排查、系统维护、技术方案实施，其中1名专注硬件及网络问题，1名专注软件及数据问题。

(3)运维工程师（2名）：3年以上客户服务经验，负责问题接收、分类、跟踪及结果反馈，管理服务档案，定期回访用户满意度。

9. (4)业务咨询专员（2名）（熟悉政务服务业务） 团队成员全程投入项目，不兼任其他项目核心角色。



11.3.3 团队稳定性保障

人员锁定机制：项目验收后，售后服务核心成员（总负责人、技术支持组长、业务咨询组长）需稳定服务至少1年，期间不得随意更换；若因特殊情况（如离职、重大疾病）需更换，需提前15天向濮阳市政府办提交《售后服务人员变更申请》，说明变更原因、新成员资质证明及过渡期安排，经甲方书面同意后方可更换，且新成员需通过甲方组织的能力考核（含技术实操、业务问答）。

团队培训计划：每月组织1次售后服务团队内部培训，内容包括：

政策更新培训：如政务公开新政策、政府网站建设新规范解读；

技术提升培训：如新型网络攻击防护技术、云存储服务优化技巧；

服务流程培训：如响应机制优化、问题处理规范更新；

案例复盘培训：分析典型故障处理案例，总结经验教训，提升团队整体能力。

绩效考核机制：建立以“服务质量”为核心的绩效考核体系，考核指标包括：

响应及时性：是否在承诺时限内响应问题；

问题解决率：已处理问题占总问题的比例；

用户满意度：政府工作人员对服务的评分；

安全事故数：因个人操作失误导致的安全生产事故数（目标=0）；

11..4 基础服务保障

11.4.1. 平台性能监控

(1)部署实时监控系統，对服务器 CPU 使用率（阈值 $\leq 80\%$ ）、内存占用（阈值 $\leq 85\%$ ）、磁盘空间（阈值 $\leq 90\%$ ）、平台响应时间（阈值 ≤ 3 秒）等指标进行 24 小时监测，触发阈值时自动向技术工程师推送预警信息。

11.4.2 数据安全备份

(1)采用“本地+异地”双备份机制：每日 23:00 自动执行全量备份（本地服务器存储），每周日执行增量备份（同步至异地灾备中心），备份数据保留 90 天。

(2)每月进行 1 次备份恢复测试，验证数据完整性，测试报告同步用户方。

11.4.3 历史数据迁移归档

(1)针对超过 1 年的非活跃数据，按用户需求制定迁移计划，采用加密压缩方式迁移至归档服务器，提供在线查询接口，确保数据可追溯。迁移前需经用户方确认，迁移后出具验收报告。

11.5 售后服务计划

11.5.1 短期计划

- (1) 每周进行 1 次电话回访，收集用户使用反馈，主动排查潜在问题。
- (2) 组织 1 次操作技巧进阶培训，针对常见操作误区提供解决方案。

11.5.2 中期计划

- (1) 每季度开展 1 次系统优化评估，结合用户业务增长需求，提出硬件升级或软件调优建议。
- (1) 建立用户服务群，定期分享平台使用技巧、故障处理案例。

11.5.3 长期计划

- (1) 每年进行 1 次全面服务复盘，根据用户反馈优化服务流程。
- (2) 配合用户方进行平台年度运维审计，提供所需的服务记录、备份日志等资料。

11.6 售后服务承诺

11.6.1 服务质量承诺

- (1) 严格遵守本方案所有内容，不缩减服务范围、不延长响应时间，所有服务均以用户实际需求为核心，无套用其他项目模板、凭空编造或夸大表述的情况。
- (2) 若因我方服务不到位导致用户业务受影响，愿意承担相应责任（具体按合同约定执行），并在 24 小时内提出补偿方案。

11.6.2 人员稳定性承诺

- (1) 售后服务核心团队（服务主管、技术工程师）在项目服务期内保持稳定，如需变动，提前 15 天书面通知用户方，且替代人员资质不低于原岗位标准，经用户确认后方可上岗。

11.6.3 数据安全承诺

(1)严格遵守《网络安全法》《数据安全法》，对用户数据实行“专人管理、加密传输、权限隔离”，绝不泄露、滥用用户数据，若发生数据安全事件，承担全部法律责任。

11.6.4 问题解决承诺

(1)紧急故障 4 小时内解决、重要故障 6 小时内解决、一般故障 24 小时内解决。

11.6.5 持续性服务承诺

(1)项目服务期结束后，可根据用户需求提供延续服务，服务内容与收费标准提前 3 个月协商确定，确保服务无缝衔接。

本方案及承诺均基于项目实际需求制定，所有条款均具备可操作性，无逻辑漏洞或无法实现的情形，特此承诺。

11.7 核心售后服务内容

11.7.1 平台日常运维支持

针对政府网站技术运维及运行保障服务第 1-4 项工作内容，提供全周期日常运维支持，确保平台稳定运行：

性能监控服务

监控范围：覆盖服务器、数据库、网络、应用系统 4 大维度，具体包括：

服务器：CPU 使用率、内存占用、磁盘空间、磁盘、网络带宽；

数据库：连接数、查询响应时间、表空间使用率、锁等待次数；

网络：ping 延迟、丢包率、域名解析成功率；

应用系统：页面加载时间、接口调用成功率、并发用户数。

监控工具：部署 Zabbix 监控系统，并在集约化平台后台开发“运维监控模块”，供甲方管理员实时查看监控数据。

监控频率：实时监控，内容包括：指标达标情况、异常指标分析、优化建议。

异常处理：若监控发现指标超标，运维专员 15 分钟内通知技术支持工程师，工程师 30 分钟内排查原因并优化（如清理服务器垃圾文件、优化数据库查询语句、扩容带宽），优化后 1 小时内验证效果，确保指标恢复正常。

数据安全备份服务

备份范围：包括平台所有业务数据（政务公开信息、依申请公开记录、互动留言、用户信息）、配置数据（系统设置参数、站点配置、权限配置）、附件数据（图片、文档、媒体文件）。

备份策略：

增量备份：备份前 24 小时内新增或修改的数据，备份文件存储至本地备份服务器；

全量备份：备份所有数据，备份文件同时存储至本地备份服务器及异地云存储；

备份文件保留期限：增量备份保留 30 天，全量备份保留 30 天。

1. 备份验证：每月最后一个周五 10:00-12:00 进行数据恢复测试，恢复至测试环境，验证数据完整性、准确性（与原数据一致）、可用性（可正常查询、编辑）。
2. 应急恢复：若发生数据丢失（如数据库损坏、误删除），技术支持团队立即启动《数据恢复应急预案》，优先使用最新全量备份+增量备份恢复数据，恢复过程中每 30 分钟向甲方反馈进度，确保 2 小时内完成核心数据（政务公开信息、依申请公开记录）恢复，4 小时内完成全部数据恢复，恢复后经甲方签字确认后闭环。

3. 历史数据迁移梳理及归档服务

4. 迁移后维护：针对已完成的历史数据迁移工作，每月开展 1 次数据核查，重点检查迁移数据的完整性（如是否存在字段缺失、记录遗漏）、一致性（如部门名称、栏目分类与现有平台匹配）、可用性（如历史文件可正常下载、历史互动留言可正常查看），发现问题 24 小时内修复。
5. 数据归档管理：
6. 按“年度+部门+数据类型”建立归档体系，每年 12 月协助甲方对当年非活跃数据（如 1 年前发布的非核心信息）进行归档，归档数据存储至专用归档服务器，确保可查询、可追溯。
7. 开发“历史数据查询模块”，集成至平台后台，支持甲方按部门、时间、关键词等维度快速检索归档数据，查询响应时间 3 秒。
8. 每季度对归档数据进行完整性检查，防止数据损坏或丢失，归档数据保留期限严格遵循《中华人民共和国档案法》及濮阳市政府数据管理相关规定。
9. 4. 业务配置发布及维护服务
10. 配置维护：对集约化平台应用功能（系统设置、站点管理等）和管理功能的业务配置进行日常维护。
11. 系统参数配置：每月检查系统基础信息、上传系统、第三方接口等配置是否正常，若因政策调整或第三方服务变更需修改配置（如敏感词库更新、接口密钥更换），24 小时内完成调整并测试。
12. 站点配置维护：每季度核查各部门网站域名、SSL 协议、SEO 信息、附件发布规则等配置，确保与甲方需求一致；若部门调整（如机构合并、名称变更），1 个工作日内完成站点配置修改（如域名跳转、站点名称更新）。
13. 权限配置维护：根据甲方提供的机构、人员调整通知，24 小时内完成用户组、角色、机构权限的新增、修改或删除，确保权限不越级、不混乱；每月核查 1 次权限配置，防止出现



权限冗余或缺失。

14. 配置发布支持：若甲方新增业务配置需求（如新增栏目模型、调整审核流程），业务咨询专员 1 个工作日内对接需求，技术支持工程师 3 个工作日内完成配置开发与测试，测试通过后在甲方指定时间（优先选择非工作时间）发布上线，发布后提供操作指导，确保相关人员熟练使用。

11.7.2 网站建设与维护服务

15. 对应政府网站技术运维及运行保障服务第 5-7 项工作内容，聚焦集约化平台内网站全生命周期维护，确保网站合规、高效运行：

16. 1. 部门网站建设与维护

17. 新建支持：若甲方新增部门网站建设需求，提供“需求对接-方案设计-配置开发-测试上线”全流程支持：

18. 需求对接：业务咨询专员 1 个工作日内与新增部门沟通，明确网站定位、栏目设置、功能需求（如是否需要投票问卷、内容采集功能），形成《部门网站建设需求清单》。

上线验收：配置完成后，协助部门开展内部测试，收集反馈并 24 小时内优化，优化完成后提交甲方验收，验收通过后 1 个工作日内正式上线。

19. 日常维护：

20. 内容巡检：每日配合甲方“值班读网”工作，检查部门网站内容更新情况、信息准确性、链接可用性，发现问题 1 小时内反馈对应部门，督促 24 小时内整改，并记录。

21. 功能维护：每周检查部门网站核心功能是否正常，若出现功能故障，技术支持工程师 2 小时内排查，24 小时内解决。

22. 改版支持：若部门提出网站改版需求（如模板更换、栏目调整），1 个工作日内对接需求，

3个工作日内完成改版方案设计与配置，测试通过后在非工作时间上线，确保不影响网站正常访问。

23. 2. 政务公开平台维护

24. 功能维护：每日检查政务公开平台核心功能（信息发布、检索、统计），确保：

25. 信息发布功能正常，支持按“法定主动公开内容”分类发布，字段填写符合规范（如发布时间、文号、来源）；

26. 高级检索功能可用，支持按关键词、部门、时间、信息类型等多维度组合查询，查询结果准确、无遗漏；

27. 统计功能正常，可按部门、栏目、时间维度统计信息发布量，数据与实际发布情况一致。

28. 信息编排服务：协助甲方实施市政府文件类信息编排工作：

29. 接收甲方提供的市政府文件，1个工作日内完成文件格式规范（如字体、行距、页码）、关键词提取、分类标注）；

30. 24小时内将编排后的文件上传至政务公开平台指定栏目，同步生成文件预览（支持PDF格式），确保公众可在线查看、下载；

31. 上传完成后，1小时内核查文件发布情况（是否成功显示、链接是否可用），发现问题立即修复。

32. 数据支撑：每月向甲方提供政务公开平台运行数据报告；

33. 信息发布统计：各部门月度发布量，未达标部门名单（按甲方要求的发布频次标准）；

34. 访问统计：平台月度PV/UV/IP数据、热门信息排行、访问者地区分布；

35. 问题统计：当月发现的信息错误、死链等问题数量及整改率，为甲方监管提供数据支持。

36. 3. 市政府门户网站维护

37. 日常巡检与维护：



38. 每日 8:00 前完成门户网站全量巡检;
39. 页面显示: 检查首页、栏目页、详情页是否存在布局错乱、图片失效、文字乱码;
40. 功能可用性: 测试搜索、互动交流(留言板、在线咨询)、依申请公开、文件下载等功能是否正常;
41. 链接有效性: 检查首页及核心栏目链接(如部门导航、政务服务入口)是否存在死链, 确保跳转准确。
42. 发现问题分类处理: 页面显示问题 1 小时内修复; 功能故障 2 小时内排查, 24 小时内解决; 死链问题 1 小时内反馈对应责任部门, 督促 2 小时内更新链接, 同步在网站后台标记“已修复”。
43. 内容更新支持:
44. 协助甲方更新门户网站核心内容(如首页头条、政务要闻、通知公告), 接收甲方提供的内容素材后, 2 小时内完成编辑(如排版、配图), 经甲方确认后 1 小时内发布;
45. 每月协助甲方梳理门户网站未更新栏目, 反馈至对应责任部门, 督促按时更新, 确保无长期(超过 1 个月)未更新栏目。
46. 重大活动保障: 若门户网站配合濮阳市重大活动(如政府工作报告发布、重大政策解读)进行专题改版或内容聚焦, 提前 7 个工作日对接需求:
47. 3 个工作日内完成专题页面设计、功能配置;
48. 2 个工作日内协助甲方收集、编辑专题内容, 完成上线测试;
49. 活动期间安排专人 7×24 小时值守, 实时监控网站运行状态, 确保无卡顿、无故障, 若出现突发问题, 15 分钟内响应处理。

11.7.3 安全防护服务

50. 对应政府网站技术运维及运行保障服务工作内容，构建“预防-监测-处置-复盘”全流程安全防护体系，保障平台安全运行：

51. 1. 日常安全监测

52. 实时防护开启：确保平台安全防护功能（系统防火墙、XSS/SQL 注入拦截、恶意 IP 限制）全天候开启，防护规则按安全业界通用标准每月更新 1 次，确保能拦截最新恶意攻击手段。

53. 多维度监测：

54. 攻击监测：每日查看系统防火墙记录，监测疑似攻击行为（如高频次非法登录、异常 SQL 语句请求、XSS 脚本注入），对拦截的攻击行为分类统计（按攻击类型、来源 IP、攻击时间），形成《每日安全攻击监测报告》；

55. 漏洞监测：每月使用专业漏洞扫描工具（如 Nessus）对平台进行 1 次全量漏洞扫描，覆盖服务器、数据库、应用系统、第三方组件，扫描内容包括高危漏洞（如远程代码执行、权限绕过）、中低危漏洞（如弱口令、信息泄露），形成《漏洞扫描报告》，标注漏洞等级、影响范围、修复建议；

56. 隐私泄露监测：每季度对平台内所有网站开展信息隐私泄露检查，重点排查是否存在未脱敏的个人信息、敏感政务数据，发现泄露问题 2 小时内通知对应部门，督促 24 小时内删除或脱敏处理；

57. 页面篡改监测：每日使用页面篡改监测工具，检查平台首页、核心栏目页是否被篡改，若发现篡改（如页面内容替换、植入恶意链接），立即触发告警，技术支持团队 15 分钟内响应，1 小时内恢复页面至最新备份版本，并追溯篡改来源。

58. 2. 漏洞修复与加固

59. 漏洞修复时限：

60. 高危漏洞：扫描发现后 24 小时内完成修复（如安装安全补丁、修改配置、代码加固），修复后 1 小时内验证效果，确保漏洞已消除；
61. 中危漏洞：3 个工作日内完成修复与验证；
62. 低危漏洞：7 个工作日内完成修复与验证；
63. 若漏洞修复需停机维护，提前 3 个工作日向甲方提交，说明维护时间（优先选择夜间或周末）、影响范围，经甲方同意后执行。
64. 安全加固措施：
65. 服务器加固：禁用不必要的端口（如 Telnet、FTP 默认端口）、服务（如 WebDAV），配置服务器访问控制列表（ACL），仅允许指定 IP 段访问管理端口；
66. 数据库加固：修改默认管理员账号密码（复杂度满足“大小写字母+数字+特殊字符”），定期（每月 1 次）更换密码，限制数据库远程访问，仅允许平台应用服务器连接；
67. 应用系统加固：对平台代码进行安全审计（每季度 1 次），修复代码层面的安全隐患（如未过滤用户输入、会话管理不当），配置应用级防火墙（WAF），拦截异常请求；
68. 账号安全加固：强制管理员账号启用双因素认证（如“密码+手机验证码”），设置密码有效期（90 天），对连续 5 次登录失败的账号自动锁定 1 小时，防止暴力破解。
69. 3. 应急安全处置
70. 应急预案制定：制定平台安全应急处置预案，明确不同安全事件（DDoS 攻击、数据泄露、网页篡改、病毒感染）的响应流程、责任分工、处置措施，每半年组织 1 次预案演练，确保团队熟练掌握处置流程。
71. 应急响应流程：
72. 事件发现与告警：通过安全监测工具或用户反馈发现安全事件后，运维专员立即向售后服务总负责人报告，说明事件类型、影响范围、当前状态；

73. 应急启动：总负责人 15 分钟内启动对应预案，组建应急小组（技术支持、安全、数据），明确分工（如专人负责阻断攻击、专人负责数据恢复、专人负责上报）；
74. 事件处置：
75. DDoS 攻击：立即联系云服务商开启 DDoS 高防服务，配置流量清洗规则，阻断异常流量，同时调整服务器端口策略，确保核心业务（如政务公开、依申请公开）可用；
76. 数据泄露：立即定位泄露数据来源，关闭泄露通道，删除外部泄露数据（若已扩散），同时通知受影响用户，采取补救措施；
77. 网页篡改：立即下线被篡改页面，从备份恢复正常页面，扫描服务器是否存在恶意后门，清除恶意代码，修改管理员账号密码；
78. 病毒感染：断开受感染服务器与网络的连接，使用专业杀毒软件清除病毒，备份重要数据，重装操作系统，重装后恢复数据并测试；
79. 事件上报：重大安全事件处置过程中，每 30 分钟向甲方同步进度，处置完成后 2 小时内说明事件原因、处置措施、损失评估、改进方案；
80. 复盘优化：事件处置完成后 3 个工作日内组织复盘会议，分析事件暴露的安全短板，优化应急预案与防护体系，避免同类事件再次发生。
81. 4. 安全检查与评估
82. 定期安全检查：
83. 月度检查：每月最后一个工作日开展月度安全检查，内容包括：安全防护功能开启情况、漏洞修复完成情况、管理员账号安全、日志记录完整性，提交甲方备案；
84. 季度检查：每季度开展全平台安全专项检查，重点检查：信息隐私泄露、页面严重错误、互动交流内容合规性，对发现的问题分类列出整改清单，督促相关部门 3 个工作日内整改，整改完成后进行验收；

85. 年度检查：每年 12 月联合甲方开展年度安全检查，全面评估平台安全状况（防护能力、漏洞风险、应急能力），形成报告，提出下一年度安全优化建议。

11.7.4 证书管理服务

86. 对应政府网站技术运维及运行保障服务中“SSL 证书部署和定期更新”要求，提供全周期证书管理服务，确保网站 HTTPS 加密访问：

87. 1. 证书部署服务

88. 前期准备：

89. 需求对接：1 个工作日内与甲方确认部署 SSL 证书的域名清单（包括市政府门户网站、部门网站、政务公开平台等），明确证书类型（如 DV SSL、OV SSL，优先选择 OV SSL 以提升公信力）；

90. 资料准备：协助甲方准备证书申请资料（如单位营业执照、域名所有权证明、负责人身份证明），确保资料符合证书服务商要求，避免申请驳回。

91. 部署实施：

92. 证书申请：提交资料后，跟踪证书服务商审核进度（一般 1-3 个工作日），审核通过后获取证书文件（如 .pem、.key 格式）；

93. 环境配置：技术支持工程师 2 个工作日内完成服务器环境配置；

94. 在 Web 服务器（如 Nginx、Apache）中配置证书文件路径、HTTPS 端口（443 端口）；

95. 配置 HTTP 强制跳转 HTTPS（确保用户输入 HTTP 地址时自动跳转至 HTTPS）；

96. 配置 SSL 协议版本（禁用不安全的 SSLv3、TLS1.0，启用 TLS1）

97. 形成报告，提交濮阳市政府办备案。

98. 应急恢复：若发生数据丢失（如数据库损坏、误删除），技术支持团队立即启动，优先使



用最新全量备份+增量备份恢复数据，恢复过程中每 30 分钟向甲方反馈进度，确保 2 小时内完成核心数据恢复，4 小时内完成全部数据恢复，恢复后经甲方签字确认后闭环。

99. 3. 历史数据迁移梳理及归档服务

100. 迁移后维护：针对已完成的历史数据迁移工作，每月开展 1 次数据核查，重点检查迁移数据的完整性（如是否存在字段缺失、记录遗漏）、一致性（如部门名称、栏目分类与现有平台匹配）、可用性（如历史文件可正常下载、历史互动留言可正常查看），发现问题 24 小时内修复。

101. 数据归档管理：

102. 按“年度+部门+数据类型”建立归档体系，每年 12 月协助甲方对当年非活跃数据进行归档，归档数据存储至专用归档服务器，确保可查询、可追溯。

103. 开发“历史数据查询模块”，集成至平台后台，支持甲方按部门、时间、关键词等维度快速检索归档数据，查询响应时间 3 秒。

104. 每季度对归档数据进行完整性检查，防止数据损坏或丢失。归档数据保留期限严格遵循《中华人民共和国档案法》及濮阳市政府数据管理规定。

105. 4. 业务配置发布及维护服务

106. 配置维护：对集约化平台应用功能（系统设置、站点管理等）和管理功能的业务配置进行日常维护；

107. 系统参数配置：每月检查系统基础信息、上传系统、第三方接口等配置是否正常，若因政策调整或第三方服务变更需修改配置（如敏感词库更新、接口密钥更换），24 小时内完成调整并测试。

108. 站点配置维护：每季度核查各部门网站域名、SSL 协议、SEO 信息、附件发布规则等配置，确保与甲方需求一致；若部门调整（如机构合并、名称变更），1 个工作日内完成站点



配置修改（如域名跳转、站点名称更新）。

109. 权限配置维护：根据甲方提供的机构、人员调整通知，24 小时内完成用户组、角色、机构权限的新增、修改或删除，确保权限不越级、不混乱；每月核查 1 次权限配置，防止出现权限冗余或缺失。
110. 配置发布支持：若甲方新增业务配置需求（如新增栏目模型、调整审核流程），业务咨询专员 1 个工作日内对接需求，技术支持工程师 3 个工作日内完成配置开发与测试，测试通过后在甲方指定时间（优先选择非工作时间）发布上线，发布后提供操作指导，确保相关人员熟练使用。

11.7.5 网站建设与维护服务

111. 对应政府网站技术运维及运行保障服务工作内容，聚焦集约化平台内网站全生命周期维护，确保网站合规、高效运行：
112. 1. 部门网站建设与维护
113. 新建支持：若甲方新增部门网站建设需求，提供“需求对接-方案设计-配置开发-测试上线”全流程支持：
114. 需求对接：业务咨询专员 1 个工作日内与新增部门沟通，明确网站定位、栏目设置、功能需求，形成需求清单。
115. 方案设计：技术团队 2 个工作日内完成网站架构设计、模板选型、权限配置方案，提交甲方审核，审核通过后 1 个工作日内启动配置。
116. 配置开发：3 个工作日内完成站点配置（域名、SSL、SEO）、栏目搭建、模板部署、功能集成（如内容管理、智能统计），同步开展测试，确保无功能故障。
117. 上线验收：配置完成后，协助部门开展内部测试，收集反馈并 24 小时内优化，优化完



成后提交甲方验收，验收通过后 1 个工作日内正式上线。

118. 日常维护：

119. 内容巡检：每日配合甲方“值班读网”工作，检查部门网站内容更新情况（如是否存在未更新栏目）、信息准确性（如是否有错别字、过时信息）、链接可用性（如是否存在死链），发现问题 1 小时内反馈对应部门，督促 24 小时内整改，并记录。

120. 功能维护：每周检查部门网站核心功能（内容发布、互动交流、统计分析）是否正常，若出现功能故障（如栏目无法发布内容、统计数据异常），技术支持工程师 2 小时内排查，24 小时内解决。

121. 改版支持：若部门提出网站改版需求（如模板更换、栏目调整），1 个工作日内对接需求，3 个工作日内完成改版方案设计与配置，测试通过后在非工作时间上线，确保不影响网站正常访问。

122. 2. 政务公开平台维护

123. 功能维护：每日检查政务公开平台核心功能（信息发布、检索、统计），确保：

124. 信息发布功能正常，支持按“法定主动公开内容”分类发布，字段填写符合规范（如发布时间、文号、来源）；

125. 高级检索功能可用，支持按关键词、部门、时间、信息类型等多维度组合查询，查询结果准确、无遗漏；

126. 统计功能正常，可按部门、栏目、时间维度统计信息发布量，数据与实际发布情况一致。

127. 信息编排服务：协助甲方实施市政府文件类信息编排工作：

128. 接收甲方提供的市政府文件（如通知、意见、办法），1 个工作日内完成文件格式规范（如字体、行距、页码）、关键词提取、分类标注（如按“政策法规”“规划计划”分类）；

129. 24 小时内将编排后的文件上传至政务公开平台指定栏目，同步生成文件预览(支持 PDF 格式)，确保公众可在线查看、下载；
130. 上传完成后，1 小时内核查文件发布情况（是否成功显示、链接是否可用），发现问题立即修复。
131. 数据支撑：每月向甲方提供政务公开平台运行数据报告，包括：
132. 信息发布统计：各部门月度发布量、未达标部门名单（按甲方要求的发布频次标准）；
133. 访问统计：平台月度 PV/UV/IP 数据、热门信息排行、访问者地区分布；
134. 问题统计：当月发现的信息错误、死链等问题数量及整改率，为甲方监管提供数据支持。
135. 3. 市政府门户网站维护
136. 日常巡检与维护：
137. 每日 8:00 前完成门户网站全量巡检；
138. 页面显示：检查首页、栏目页、详情页是否存在布局错乱、图片失效、文字乱码；
139. 功能可用性：测试搜索、互动交流（留言板、在线咨询）、依申请公开、文件下载等功能是否正常；
140. 链接有效性：检查首页及核心栏目链接（如部门导航、政务服务入口）是否存在死链，确保跳转准确。
141. 发现问题分类处理：页面显示问题 1 小时内修复；功能故障 2 小时内排查，24 小时内解决；死链问题 1 小时内反馈对应责任部门，督促 2 小时内更新链接，同步在网站后台标记“已修复”。
142. 内容更新支持：
143. 协助甲方更新门户网站核心内容（如首页头条、政务要闻、通知公告），接收甲方提供

的内容素材后，2 小时内完成编辑（如排版、配图），经甲方确认后 1 小时内发布；

- 144. 每月协助甲方梳理门户网站未更新栏目，反馈至对应责任部门，督促按时更新，确保无长期未更新栏目。
- 145. 重大活动保障：若门户网站需配合濮阳市重大活动（如政府工作报告发布、重大政策解读）进行专题改版或内容聚焦，提前 7 个工作日对接需求：
- 146. 3 个工作日内完成专题页面设计、功能配置（如专题导航、信息聚合、在线互动）；
- 147. 2 个工作日内协助甲方收集、编辑专题内容，完成上线测试；
- 148. 活动期间安排专人 7×24 小时值守，实时监控网站运行状态，确保无卡顿、无故障，若出现突发问题，15 分钟内响应处理。

11.7.6 安全防护服务

- 149. 对应政府网站技术运维及运行保障服务第 10-13 项工作内容，构建“预防-监测-处置-复盘”全流程安全防护体系，保障平台安全运行。
- 150. 1. 日常安全监测
- 151. 实时防护开启：确保平台安全防护功能（系统防火墙、XSS/SQL 注入拦截、恶意 IP 限制）全天候开启，防护规则按安全业界通用标准（如 OWASP Top 10）每月更新 1 次，确保能拦截最新恶意攻击手段。
- 152. 多维度监测：
- 153. 攻击监测：每日查看系统防火墙记录，监测疑似攻击行为（如高频次非法登录、异常 SQL 语句请求、XSS 脚本注入），对拦截的攻击行为分类统计（按攻击类型、来源 IP、攻击时间）；
- 154. 漏洞监测：每月使用专业漏洞扫描工具（如 Nessus）对平台进行 1 次全量漏洞扫描，



覆盖服务器、数据库、应用系统、第三方组件，扫描内容包括高危漏洞（如远程代码执行、权限绕过）、中低危漏洞（如弱口令、信息泄露），标注漏洞等级、影响范围、修复建议；

155. 隐私泄露监测：每季度对平台内所有网站开展信息隐私泄露检查，重点排查是否存在未脱敏的个人信息（如身份证号、手机号、家庭住址）、敏感政务数据（如未公开的统计数据、内部文件），发现泄露问题 2 小时内通知对应部门，督促 24 小时内删除或脱敏处理；

156. 页面篡改监测：每日使用页面篡改监测工具（如定期截图比对、文件哈希值校验）检查平台首页、核心栏目页是否被篡改，若发现篡改（如页面内容替换、植入恶意链接），立即触发告警，技术支持团队 15 分钟内响应，1 小时内恢复页面至最新备份版本，并追溯篡改来源。

157. 2. 漏洞修复与加固

158. 漏洞修复时限：

159. 高危漏洞：扫描发现后 24 小时内完成修复（如安装安全补丁、修改配置、代码加固），修复后 1 小时内验证效果，确保漏洞已消除；

160. 中危漏洞：3 个工作日内完成修复与验证；

161. 低危漏洞：7 个工作日内完成修复与验证；

162. 若漏洞修复需停机维护，提前 3 个工作日向甲方提交，说明维护时间、影响范围，经甲方同意后执行。

163. 安全加固措施：

164. 服务器加固：禁用不必要的端口（如 Telnet、FTP 默认端口）、服务（如 WebDAV），配置服务器访问控制列表（ACL），仅允许指定 IP 段访问管理端口；

165. 数据库加固：修改默认管理员账号密码（复杂度满足“大小写字母+数字+特殊字符”），定期（每月 1 次）更换密码，限制数据库远程访问，仅允许平台应用服务器连接；



166. 应用系统加固：对平台代码进行安全审计（每季度 1 次），修复代码层面的安全隐患（如未过滤用户输入、会话管理不当），配置应用级防火墙（WAF），拦截异常请求；
167. 账号安全加固：强制管理员账号启用双因素认证（如“密码+手机验证码”），设置密码有效期（90 天），对连续 5 次登录失败的账号自动锁定 1 小时，防止暴力破解。
168. 3. 应急安全处置
169. 应急预案制定：明确不同安全事件（DDoS 攻击、数据泄露、网页篡改、病毒感染）的响应流程、责任分工、处置措施，每半年组织 1 次预案演练，确保团队熟练掌握处置流程。
170. 应急响应流程：
171. 事件发现与告警：通过安全监测工具或用户反馈发现安全事件后，运维专员立即向售后服务总负责人报告，说明事件类型、影响范围、当前状态；
172. 应急启动：总负责人 15 分钟内启动对应预案，组建应急小组（技术支持、安全、数据），明确分工（如专人负责阻断攻击、专人负责数据恢复、专人负责上报）；
173. 事件处置：
174. DDoS 攻击：立即联系云服务商开启 DDoS 高防服务，配置流量清洗规则，阻断异常流量，同时调整服务器端口策略，确保核心业务（如政务公开、依申请公开）可用；
175. 数据泄露：立即定位泄露数据来源（如数据库漏洞、文件权限不当），关闭泄露通道，删除外部泄露数据（若已扩散），同时通知受影响用户（如涉及公众个人信息），采取补救措施；
176. 网页篡改：立即下线被篡改页面，从备份恢复正常页面，扫描服务器是否存在恶意后门，清除恶意代码，修改管理员账号密码；
177. 病毒感染：断开受感染服务器与网络的连接，使用专业杀毒软件清除病毒，备份重要数据，重装操作系统（若病毒无法彻底清除），重装后恢复数据并测试；

178. 事件上报：重大安全事件处置过程中，每 30 分钟向甲方同步进度，处置完成后 2 小时内说明事件原因、处置措施、损失评估、改进方案；
179. 复盘优化：事件处置完成后 3 个工作日内组织复盘会议，分析事件暴露的安全短板（如防护规则不足、监测不及时），优化应急预案与防护体系，避免同类事件再次发生。
180. 定期安全检查：
181. 月度检查：每月最后一个工作日开展月度安全检查，内容包括：安全防护功能开启情况、漏洞修复完成情况、管理员账号安全（如是否存在弱口令）、日志记录完整性提交甲方备案；
182. 季度检查：每季度开展全平台安全专项检查，重点检查：信息隐私泄露、页面严重错误、互动交流内容合规性），对发现的问题分类列出整改清单，督促相关部门 3 个工作日内整改，整改完成后进行验收；
183. 年度检查：每年 12 月联合甲方开展年度安全检查，全面评估平台安全状况（防护能力、漏洞风险、应急能力），提出下一年度安全优化建议（如升级防护工具、增加安全培训）。
184. 对应政府网站技术运维及运行保障服务中“SSL 证书部署和定期更新”要求，提供全周期证书管理服务，确保网站 HTTPS 加密访问：
185. 1. 证书部署服务
186. 前期准备：
187. 需求对接：1 个工作日内与甲方确认部署 SSL 证书的域名清单，明确证书类型；
188. 资料准备：协助甲方准备证书申请资料（如单位营业执照、域名所有权证明、负责人身份证明），确保资料符合证书服务商要求，避免申请驳回。
189. 部署实施：
190. 证书申请：提交资料后，跟踪证书服务商审核进度（一般 1-3 个工作日），审核通过后

获取证书文件（如.pem、.key 格式）；

- 191. 环境配置：技术支持工程师 2 个工作日内完成服务器环境配置，包括：
- 192. 在 Web 服务器（如 Nginx、Apache）中配置证书文件路径、HTTPS 端口（443 端口）；
- 193. 配置 HTTP 强制跳转 HTTPS（确保用户输入 HTTP 地址时自动跳转至 HTTPS）；
- 194. 配置 SSL 协议版本（禁用不安全协议 SSLv2、SSLv3、TLS1.0，启用 TLS1.1、TLS1.2）；

供应商名称（盖章单位公章）：濮阳濮阳报信息技术有限公司

法定代表人或授权委托人（签字或盖电子签章）：

赵建军

2025 年 09 月 01 日