中国中医科学院西苑医院

互联网门户系统升级项目需求描述

网站需要实现中国中医科学院西苑医院大众版、专业版、国际版、国家中医心血管病临床医学研究中心网站点群的格局建立和管理，页面设计需符合中国中医科学院西苑医院互联网品牌形象，统一风格和样式管理，栏目架构制定符合医院及各部门需求需要，网站需要预留拓展功能开发接口及模块。

一、医院官方门户内容管理系统

网站需实现内容管理，内容管理包含网站群的文章、图片、公告、友情链接、留言、转向链接、Flash、视频等。

1.内容模型包含：文章模型、图片模型、软件模型、公告模型、友情链接模型、留言模型、转向链接模型、Flash模型、音乐模型、视频模型等。网站可发布素材包括：图片（首页banner图轮播、文章内图片、医生照片等）、音/视频文件素材（MP3、MP4、flash等）、附件上传（xlsx/xls、docx/doc等格式并支持正常下载）、文字素材。

2.信息管理要求提供信息的标题、副标题、引题、链接标题的编辑。支持XML格式数据的批量导入与导出。发布管理可以发布、撤销及重新发布信息。支持同一篇文章信息同时发布在不同的栏目中。

3.信息发布与审核功能要求：

（1）编辑器要求系统含图文混排，支持带Word图片上传功能，并且支持同一篇文章同时发布到多个栏目和站点。

（2）信息审批发布中可以编辑、新建流程、指定流程节点人员，建立不同栏目的信息发布审批流程。系统支持自定义审核流程、自定义的后台菜单功能。

（3）关键词过滤：发布文章时系统能对设置关键字进行过滤，并根据需要过滤的字符设置好替换目标、优先级状态等信息。充分利用模式匹配信息，加快跳跃幅度，提高匹配的速度。

（4）支持文章定时器发布功能；支持文章发布分权限浏览设置功能。

（5）栏目管理可实现栏目的新增、删除、编辑、移动、排序等功能；栏目的类型可支持信息发布类型、虚拟栏目类型、链接类型、文件下载类型等格式。

（6）支持静态页部署；提供专业的静态页面生成方式，如“.html”“.htm”“.shtml”“.shtm”。

（7）内置“全文检索引擎系统”，全文检索引擎具备多关键字搜索、关键词组合搜索、全文检索（对文章标题，文章关键词、作者、发布时间同时检索）等功能，能快速准确地检索到网站内的所有信息，并对关键词进行高亮显示。

（8）模板管理：应采用网页模板与程序分离的技术，可以通过不断地调整网页模板的设置或更改模板来完成网站的风格改版和更新。

（9）信息采集：应采用多项目管理，针对不同的采集源可以设置多个采集项目，并对采集项目进行采集规则的定义，系统提供二次开发接口处理内容的本地化。

（10）用户登录。支持双因子认证并支持多种登录方式，包括：微信扫码登录、手机号快捷登录、账号登录等。检测到非常用IP登录要求手机验证，登录长时间无操作自动退录。

（11）分权限管理：高层级管理员可对低层级管理员所发布的内容进行编辑修改和删除。

（12）要可视化的页面编辑功能：即后台操作员登录后，浏览前台页面时可以直接可视化编辑页面中的任何内容，包括并不限于：焦点图、任意位置的图标、图片、背景图、视频、文字、以及对应的链接等。

4.审核流程及用户权限要求

（1）系统应支持网站内容多级、逐级审核机制。

▲（2）实现网站内容同源管理。系统可清晰实现图文内容为同源根内容或同源分支内容，并具备完善的编辑和审核机制。子网站/频道/栏目中的内容也可以推荐给主网站/其他子网站/频道或栏目，在对应权限的管理员审核后使用。

（3）系统须提供内容发布智能触发机制，包括：图文内容的定时发布/定时审核/定时撤销发布等。

5.国际版内容站点设立

网站需要实现页面全外文展示，并支持独立多语种网站配置，可实现独立的外文频道和栏目设置，页面样式符合国际网站建设和设计风格。

▲6.分中心网站点群的格局建立和管理

需要实现以中心概况、新闻中心、临床医疗、科学研究、辐射推广、人才培养功能为主的国家中医心血管病临床医学研究中心平台建立，搭建对应内容及项目展示站点，支持联盟在线病例讨论、全局搜索、分中心信息管理。中心网站建设应在30个工作日内完成建设并部署上线。（响应文件中应出具初步方案、承诺函。）

二、建立医院自有的医生、科室、疾病数据库

1.建立网站医生信息库，实现医生科研教学和医疗服务信息的综合展示，支持医生信息与科室、疾病、文章等关键信息关联查询和展示。

2.建立网站科室信息库，实现科室信息独立维护管理，支持科室信息与医生、疾病、文章等关键信息关联查询和展示。

3.建立网站疾病信息库，实现疾病信息与科室、医生信息进行关联查询和展示。

▲4.实现科室展示的后台排序设置；实现医生在全院、科室、疾病分类和搜索结果的排序可设置。

▲5.支持科室页和医生页生成科室名片和医生名片，用户可通过扫描科室名片或医生名片的二维码的方式访问页面。

▲6.科室医生疾病页能与医院出诊大表进行关联，并在科室页和医生页展示科室和医生的出诊信息；支持各种类型的停诊设置（近期停诊、长期停诊）和展示。

三、出停诊及排班管理

▲1.实现完全系统管理的门诊出停诊排班表。支持一次设置（出诊或停诊信息），所有涉及的排班信息（包括出诊大表、科室站点排班表、专家站点排班表）自动更新。

▲2.支持各种类型出停诊展示模式，包括：多院区出诊、专家团队出诊、会诊模式、专病出诊、特需门诊等。

3.支持门诊科室的系统化设置，包括：门诊科室与住院科室的关联、门诊诊室（楼层）设置等；

▲4.支持门诊各类停诊设置，包括：近期停诊与长期停诊规则设置、单日或单次停诊、阶段性停诊设置、跳跃性停诊设置等。

▲5.支持出诊信息的跨平台展示，包括：轻应用、响应式（各类移动端浏览器）。

四、移动门户网站及微信对接

1.将移动门户与医院门户网站进行无缝整合，移动门户与医院网站共享数据信息。

2.兼容主流浏览器（IE、chrome、Safari），尤其是手机浏览器，保持其完整性和美观。

▲3.实现响应式设计，适配PC、手机、Pad各种设备，且保证在各电子终端上可正常浏览（包括清晰度和加载速度），以保证网民浏览习惯和访问体验。

▲4.微信与网站数据同步，并支持医院微矩阵和智能知识库搜索和互联网平台的即时切换。

五、人事招聘功能

实现在线招聘功能，包括：应聘人员注册、在线申请，实现招聘岗位信息发布，招聘简历管理（电子简历打印/批量打印，简历信息批量excel导出，招聘简历数据接口输出等），通知等功能。

六、数据迁移

对现有网站历史数据实现迁移，包括但不限于用户数据，文章数据，视频数据，预约就诊信息等。实现新旧网站迁移的平稳过渡。

1.新版网站搭建完成后，需根据网站不同栏目、频道数据特点，采用不同的迁移方式，确保迁移后的数据完整性、一致性。

2.对于数据映射比较规则的数据，采用数据迁移工具软件实现自动迁移整合，实现单项或批量数据迁移。

3.对映射关系不规则的数据，采用手工迁移整合，实现单项或批量数据迁移。最后需提供迁移数据完整性、一致性检测工具，保证数据迁移的质量。

七、平台安全管理功能

▲1.网站访问异常提醒功能：对门户网站运行状态进行实时监测，一旦运行状态出现异常，系统将向指定的联系方式（电子邮件、手机短信等）发送异常提醒消息，提醒相关管理人员；（须提供功能截图并加盖公章）

▲2.要求有网站实时监测功能，可以监测网站实时运行状态，定期对网站代码实时扫描，每次代码升级更新也要对网站代码实时扫描，避免高危漏洞。

3.要有数据传输安全策略，对医院所有数据进行加密处理，去隐私化。

4.系统须具备密码安全管理功能：弱口令的禁止，对网站所有密码要有定期强制修改机制。

▲5.用户名密码安全管理。系统可设置用户名密码安全等级，并可进行后台设置，实现强密码要求设置

▲6.敏感词查验：非法字符查验和自定义关键词查验。平台系统要具备对网站中的信息进行全网筛查功能。

▲7.实现门户网站系统一键重启、关闭、升级、锁定功能。

8.系统需具备完整的日志管理，应记录有系统核心产生的错误信息，应记录应用程序产生的错误信息，应记录管理员在后台的操作、活动信息；对于系统主要数据信息（科室、医生、疾病、排班、文章、视频等）的修改能够对前后内容进行完整的对比记录；

9.网站具备有效的应用安全防护，代码健壮，能够有效防护SQL注入和跨脚本攻击。

10.URL参数安全过滤：用户可以自由设置URL可传递的参数个数、类型等，或者选择是否开启。并通过限制URL参数传递的方式来进行安全过滤，从而杜绝SQL注入等黑客攻击方式。

11.IP访问限定功能：设置限定访问网站客户的IP信息，包括：全站来访限定方式、全站IP段白名单和黑名单、后台来访限定方式、后台IP段白名单和黑名单等信息。

12.支持SSL加密通信：系统支持部署在SSL加密通信环境中。

▲13.页面防篡改。系统具备页面防篡改监测提醒功能，并且具备当页面发生非系统允许操作的改变时，系统将自动以短信或email等方式通知备注管理人员。

八、性能要求

1.对关键数据采取访问权限限制。能保证数据的完整性、一致性和有效性。应采用严格的操作员身份认证机制，防止伪造身份人员冒用系统资源。

2.系统应在长时间运行下仍能顺畅访问，保证网站每天能够正常使用。

3.后台操作响应时间符合正常使用要求。

4.云服务器参数：

规格：≥8核 | ≥16GB

系统盘：SSD硬盘｜ ≥100GB

数据盘：SSD硬盘｜ ≥500GB

弹性公网IP：全动态BGP | 独享 | 按带宽计费 | 15Mbit/s

5.云安全配置要求：

1）Web应用防火墙

支持常见的Web攻击防护，包括XSS攻击、SQL注入等，支持HTTP和HTTPS的业务防护（支持10个端口转发，不限于80、8080、443、7443、8443端口）。

2）企业主机安全服务（HSS）

A.主机安全防护：提供企业级主机安全防护全部功能。

B.静态网页防篡改：防止网站服务器中的静态网页文件被篡改。

C.网盘文件防篡改：防止共享文件网盘中的网页文件被篡改。

D.资产管理：账号信息管理、开放端口检测、进程信息管理、Web目录管理、软件信息管理。

E.漏洞管理：Linux软件漏洞管理、Windows系统漏洞管理、Web-CMS漏洞管理。

F.入侵检测：双因子认证、账户破解防护、异地登录检测、关键文件变更检测、恶意程序检测、网站后门检测。

G.基线检查：口令复杂度策略检测、经典弱口令检测、风险账号检测、配置检测。

3）OBS

对象存储服务 OBS（Object Storage Service）具备标准Restful API接口，可存储任意数量和形式的非结构化数据。

4）SSL证书服务

加密强度40位至256位自适应对称加密算法，2048位RSA公钥（非对称加密算法）。

支持通配型域名：支持\*.domain.com，同一台物理服务器下的子域数量不限。

支持双域名：一张证书免费同时支持两个相关域名（www.和没有www.)。

支持证书状态在线查询协议（OCSP)。

支持证书吊销列表（CRL)。

九、平台接口及拓展管理

▲网站系统提供标准的整合接口文档，并有成熟的整合和集成经验，满足医院网站发展需要，能够预留接口进行后期功能开发模块。

▲1.建立统一的医院内外网数据交互通道，通过统一接口层获取数据与外部系统联接、获取数据并向各子业务系统提供XML数据格式包。

2.系统提供SMTP和POP3标准接口，支持邮箱认证或通知功能。

3.系统提供第三方短信通道接口，支持短信验证、找回密码、短信通知、提醒等功能。

4.系统须具备xml信息接口，支持通过xml接口向第三方网站平台的数据上报和数据输出。

5.系统具备成熟的医院内外网数据交互机制，支持与HIS、LIS、PACS等医院内信息系统的webservice接口和文件交换接口，并支持数据安全加密。

6.系统支持与第三方互联网、移动互联网平台的接口，包括：微信、支付宝等。

7.预留各类拓展功能模块，如检查检验结果查询等便民惠民服务。

十、运维管理

网站建站及使用期间，至少保证3年的长期运维服务和技术支持，如协助医院设计专题图片、网站内容更新、栏目添加删减、BUG修复、医生及出诊信息变更、软件版本升级，系统基础故障解决等。

1.图文编辑排版服务、媒体美工设计支持服务。

2.每周人工安全监测，需有专业人员每周登录服务器进行检测，检测内容不限于：网站磁盘占用情况；网站目录异常文件；检查数据库有无异常情况；检查日志系统是否有异常。

▲3.定期对日志进行分析，至少每月一次，及时整改发现的问题。

4.数据备份：网站文件每月完整备份，每天差异备份；数据库每日至少一次完整备份，每小时差异备份；要有分级备份存储机制。

5.定期出具网站自查安全报告。至少每月一次，安全报告内容包括但不限于：网站监测安全报告，网站访问安全报告，安全建议和整改方案。

6.系统数据代维服务、日常网站技术支持服务。

7.针对日常网站使用情况，定期出具使用建议。重大活动、重大节日等时期，需有专人进行值守，提前2周制定网站监控及故障处理预案。

8.服务器代运维服务，根据网站运行需求，对服务器端配置进行建议和操作。

9.需具备长期服务的能力，定期升级和维护系统，能及时响应院内的维护需求，保障功能顺畅使用；应具备功能扩展开发的能力，能有力支撑医院的功能升级和开发需求。

▲10.须定期（每半年）提供网站运维服务工作报告，详细记录网站在运维过程中的工作信息，包括：

1）运维需求接收的时间、对接人、内容；

2）运维需求的处理意见，服务方负责人，处理结果；

3）运维服务对不同的服务类型进行分类记录和统计。

十一、培训要求

需指派技术工程师对网站系统后台操作相关人员（不限人数）进行现场培训，培训周期根据甲方需求确认。提供各类操作文档，确保相关人员操作无误。

十二、应急响应服务

1.因CMS引起的故障或其它异常情况发生后，2小时内响应，一般性故障4小时内解决；重大故障8小时内解决；必要时须2小时内提供现场支持服务，提供硬件故障备机。

2.遇国家法定节假日、重大活动，提前2周制定网站监控及故障处理预案，并书面提交甲方。提供重大保障期间的应急响应人员名单。

3.故障或异常情况处理完毕后立即向甲方提交故障或异常情况处理的书面报告。

十三、等保相关

1.通信传输

1. 应采用校验技术或密码技术保证通信过程中数据的完整性；
2. 应采用密码技术保证通信过程中数据的保密性。
3. 身份鉴别和访问控制
4. 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
5. 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
6. 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
7. 应对登录的用户分配账户和权限；
8. 应授予管理用户所需的最小权限，实现管理用户的权限分离；

2.安全审计

1. 应具备安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
2. 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
3. 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

3.入侵防范

1. 应遵循最小安装的原则，仅安装需要的组件和应用程序；
2. 应关闭不需要的系统服务、默认共享和高危端口；
3. 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
4. 对发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

4.数据完整性

应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

5.数据保密性

应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

6.数据备份恢复

1. 应提供重要数据的本地数据备份与恢复功能；
2. 应提供重要数据处理系统的热冗余，保证系统的高可用性。

7.剩余信息保护

应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

8.网站程序安全

1. 网站在开发过程中要选择安全的语言，不使用危险函数；
2. 保障网站后台安全，分配好后台管理权限
3. 注意网站程序各方面的安全性测试，包括防止SQL注入、密码加密、数据备份、使用验证码等方面，加强安全保护措施。
4. 定期对应用与系统进行漏洞扫描，对发现的漏洞及时修复。
5. 部署杀毒软件定时对系统进行全面查杀。
6. 配置健全的安全策略，并定期核查，在不影响使用的前提下，将相关应用权限降至最低
7. 加强密码策略，密码必须符合复杂度要求，提高密码长度最小值，缩短密码最长留期。

9.其他安全

1. 应制定处置系统漏洞、计算机病毒、网络攻击、网络入侵等不同事件的应急预案
2. 应加强人员网络安全意识培训，强化保密意识和安全意识。
3. 若使用的操作系统、中间件、开发框架等被曝出0day漏洞，应及时进行修复，防止漏洞被利用。

十四、其他需求

1.备案协助，根据相关政策法规提供公安备案、工信部备案的新增备案、变更备案等相关操作。（响应人需提供2019年至今2家三甲医院备案证明。）

2.服务期间，如需到现场解决的问题，按照双方协商的时间，到现场解决问题，保障系统正常运行。

#3.协助医院做好各级检查，做出协助技术分析并出具运维报告。（响应人需提供2019年至今2家三甲医院运维报告。）

#4.多门户网站系统与自媒体平台运营推广结合，提供并建立多面的内容展示服务，运营推广期不少于180天，运营推广期内，按医院需求提供运营推广内容。（响应人需出具相应承诺函。）

#5.多门户网站系统的长期服务能力。（响应人需出具多门户网站系统的3年免费质保承诺函。）