#  需求分析

## 基础设施需求

此次项目建设采用全媒体网站管理平台的部署及发布工作，

包含数据安全、网页防篡改等。

## 业务功能需求（新建）

我院已经过多年信息化建设与积淀，覆盖医院主站、职能部门、等，基本满足医院、部门、科室信息发布的需求、科研及学术工作的需求。

但随着医院网站平台建设水平与管理质量的逐步提升，网站一方面作为信息发布、内容传递的重要媒介，同时大量出现面向部门、科室的轻应用服务需求亟需快速支撑满足。另外，信息技术始终处于快速发展中，新技术层出不穷，网站安全问题变化多样，使得医院网站管理平台面临的安全威胁越来越严峻。

基于上述的情况，申请建设我院网站管理平台，在我院网整体规划框架下，主要需求分析如下：

1. 对院门户网站PC端及移动端进行改版。
2. 对院网站进行设计实施，提升医院整体网络形象。
3. 建设网页防篡改系统，避免网页篡改问题的出现。
4. 数据完整迁移。将原平台中的网站及数据进行迁移，在迁移过程中，实行科学严谨的迁移规划，保障原有网站数据的无损性、安全性，杜绝数据丢失的现象发生。
5. 保证网站的安全发布。

### 网站管理平台

院网站管理系统，需具备实现管理机完整的化特性，可以通过国产化认证、微服务化、动态应用支持应对院大批量、多样化的网站建设需求。

针对本次项目中的医院体系，在现有基础之上，实现性能的大幅度升级，实现网站的动态横向扩张，确保站点在统一平台体系下建设的同时，仍旧实现数据的高效互通共享，前端的积极快速响应。

* **纵深的安全防护体系建设，响应国家等级保护要求**

在整体网站群发展过程中，融合新的安全技术，不断升级产品的安全体系，搭建纵深的安全防护体系，从内到外多个维度，保障站群整体安全。针对站群安全管理，采用集中管理的模式，将系统所有的安全信息以及安全管理功能，纳入统一的安全中心，进行总体管理。有效杜绝安全管理过程中，顾此失彼的现象发生。平台整体需满足IPV6的支持要求，确保了产品的代码级别的安全。安全建设上也需融入权限的三级分立、数据加密、身份认证、信息安全、主动管理等多种安全管理技术与概念，帮助信息中心，更好的从多维度最便捷高效的完整网站的安全管控。

* **国家护网重保工作台建设，提供攻防监控抓手工具**

本次项目，需打造医院的专属的重保工作台，将护网行动中需要的数据，实现全面的汇聚，建设有效的重保攻防演练管理工具，针对当前的行为操作痕迹，进行深度的记录。同时针对系统文件进行实时监控，发现问题采用有效预警和及时应对。

* **全媒体群统一，管理模式升级**

通过统一平台实现PC站、手机站、微信公众号、等多个新媒体信息发布渠道全面覆盖，统一管理客户内宣外宣两张网。同一篇稿件在网站编辑器创作之后，可以直接投递到微信的引用资源池当中，提高资源整体利用率、按照不同媒体渠道的内容生产要求，丰富样式之后直接发布，提升客户多媒体渠道发布效率，打造内宣及外宣新闻媒体渠道权威性。

* **网站一键关停，响应效率大幅提高**

网站管理平台需为我院提供更好的应急功能，通过系统内置一键关停，当前网站被关停后网站就无法进行正常访问，同时如果需要启动，点击一键启用即可对关停的网站进行恢复。

* **专业的应用管理中心赋能，保障网站深度应用安全**

全媒体应用开放平台可实现对互动应用的统一高效管理，减少二次开发成本，同时简化用户操作和管理流程。

全媒体应用开放平台为应用管理可以实现应用的多元化管理，实现应用中心的一键关停功能，对应用开放平台进行暂停服务，但不会影响网站的使用和运行，使得信息发布与应用管理并行运行，且互不干扰。同时进一步简化二级部门对应用的管理和使用过程。

### 医院网站改版建设

网站作为医院重要的宣传窗口，承载展示形象、宣传文化的重任。为了让医院网站适应新时代下发展，更好的发挥网站传播医院风采、凸显独有文化底蕴等作用。本次要求对门户网站进行定制设计及安全迁移，做到主题清晰，突出网站的专业性、服务性、丰富性，达到提升医院影响力并提升网站安全性的目的。提升医院整体网络形象。

### 网页防篡改系统

杜绝攻击者利用权限配置不当以及操作系统中间件数据库的漏洞，直接篡改网页文件；

杜绝攻击者攻击网站后台管理程序，通过篡改网页模板文件等手段造成网站系统新生成的网页文件中包含黑链、恶意代码、不当信息等有害内容；

杜绝攻击者对网站进行恶意访问，发起SQL注入等应用层攻击，造成网站数据库中的数据被篡改。

保证文件安全，内容安全，操作安全。

达到实时阻止网页篡改行为，禁止访问被篡改网页，修复被篡改的网页。

### SSL证书

要求提供SSL 证书，使网站能够进行加密传输，全面提升医院网站的传输安全性。

## 非功能性需求

### 性能需求

#### 性能指标

1、Web发布服务器在并发用户数≤200时，页面响应≤1秒；

2、网站后台管理系统的响应速度在50用户并发访问时，页面响应时间≤ 1 秒；

3、前端静态页面生成响应时间不超过3s。系统上线后，招标方可对以上速度响应指标进行实际测试检验；

4、网页数量>20000，站内关键词检索时间不超过10ms。

5、提供https协议进行访问，并保证不出现访问不安全性提示。

#### 响应指标

系统应具有良好的稳定性及多种性能保障措施，可保障全年7×24小时的连续运行，系统每年平均故障时间小于24小时，系统平均故障修复时间小于30分钟。

### 接口需求

要求能够提供标准化的API接口，保障系统的对接能力,

### 开发语言需求

要求采用PHP 语言开发，保障系统后台的灵活可变性。

###  UI求

要求提供操作便捷，浏览舒适的UI设计。

## 安全需求

### 网络安全需求

依据GB/T 22240-2020《网络安全等级保护定级指南》、GB/T 22239-2019《网络安全等级保护基本要求》等相关标准和要求，描述清楚该信息系统涉及的网络部署环境，是否具备相关的安全防护能力，如何保障新建应用系统的安全等。

#### SSL证书

要求提供加密传输通道，适配SSL证书，保障网站的安全传输及访问。

#### Web应用防火墙

具备语义分析引擎、BOT防护引擎、威胁情报引擎、行为分析引擎、基础特征引擎等五大核心检测能力，通过主动防护与被动安全相结合的方式识别可疑、已知、未知安全威胁，能够学习和识别未知的攻击模式，并自适应和调整防御策略，实现极低的误报率和优秀的0day防护能力，建立全面的安全防护体系，实现更高效、更合规、更稳定的Web应用安全保障。

支持HTTPS站点SSL算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果。

支持客户端安全防护，插入特殊的HTTP报头以保护客户端免受某些攻击包括但不限于增加以下安全报头：X-Frame-Options（用于防护客户端免受Clickjacking攻击）、X-Content-Type-Options（以防止浏览器将文件解释为内容类型声明以外的其他内容）、X-XSS-Protect（用于当检测到XSS攻击时，指示浏览器停止加载页面）、Content-Security-Policy（用于降低浏览器上的XSS风险和数据注入攻击）。

内置对SQL注入、XSS攻击检测的语义分析规则。

支持根据细粒度条件对CC攻击进行检测和防护；匹配条件由URL参数、请求头部字段、目的IP、请求方法、地理位置组成；测量指标由请求速率、请求集中度、请求离散度组成；客户端检测对象由IP、IP+URL、IP+User\_Agent等参数组成；支持从请求头字段获取真实源IP地址。

支持针对单个接口配置IP地址池、支持反代模式下后端连接使用IP地址池中的IP作为源地址进行轮询，支持不同目的的网络配置不同网关的策略路由。

#### 运维审计系统

结合各类法律法规(如等级保护、企业内控管理、分级保护等)对运维审计的要求，集身份认证(Authentication)、账户管理(Account)、控制权限(Authorization)、日志审计(Audit) 于一体，支持多种字符终端协议、文件传输协议、图形终端协议、远程应用协议的安全监控与历史查询， 具备全方位运维风险控制能力的统一安全管理与审计系统 。

支持系统升级后，再回退至升级前的版本；方便处理割接过程中出现的突发情况。

#### 综合日志审计分析

通过对网络设备、安全设备、主机和WEB应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，确保网站业务的不间断运营安全。

具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。

支持监测目标主机的CPU利用率、内存使用率、硬盘使用率、硬盘使用情况、流量等信息。

内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为6大类50+子类的安全分析场景。

### 数据安全需求

从数据的传输安全、数据加密、数据脱敏、数据分级、数据备份恢复等多个方面提供数据安全保障，从而保证数据传输载体安全性、数据本身安全性及数据获取安全性。

做好严格的访问控制策略，保证数据对各政府部门内部开放，防止越权使用造成的数据丢失、损毁等进行描述。

#### 日志管理中心

平台需要提供重保护网时期的工作台，实现重点操作监控及详细的日志跟踪，方便护网工作人员及时发现问题，提升护网效率。

#### 系统文件监控

平台需要提供重保护网时期的工作台，实现重点操作监控及详细的日志跟踪，方便护网工作人员及时发现问题，提升护网效率。

#### 系统运维监控

要求支持查看服务器运行状态，了解资源使用情况。可以展示服务器CPU、内存、应用内存使用状态。支持查看和导出历史使用状态数据。

### 应用安全需求

说明：各系统用户角色和访问权限的分配管理，在访问权限上，授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。对有敏感标记的重要信息
源应依据安全策略严格控制。

提供对数据不同层次等级的可访问能力。同时，做好密码控制、提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计和日志监控工作，通过多种手段保证应用系统的安全性。

对于应用软件自身，应具有和好的软件容错性，提供数据的有效性校验和自动保护功能。

#### 安全防护控制

要求提供系统安全防护控制功能，从系统防火墙、应用防火墙、用户访问控制等维度进行网站群系统防护功能控制。

提供安全防护控制至少包含文件防火墙、sql语法检查、注入防火墙、xss防火墙、dwr防火墙、网站访问IP封禁、账号冻结、强制修改密码、弱密码等防护项目。其中安全防护功能可以根据开启状态进行筛选。

#### 权限控制

要求系统支持分级、细粒度的权限划分，功能权限分配可详细到每一个菜单，内容管理权限可以细化到对每一个栏目的不同操作。可设置系统级别和部门级别角色，每个角色具备不同的权限，能够针对角色指派成员。

要求支持文章或栏目访问权限管理，可以设置配置对应的访问权限IP规则或可访问角色。

## 运行管理需求

### 运行维护

1.7×24小时值班

制定技术服务人员的值班制度，提供7×24小时的技术支持服务。对于售后服务请求，在30分钟内响应，必要情况下12小时内到达现场，常规技术故障在12小时内解决升级服务：在质保期内提供免费升级服务；

2.服务响应

在需要提供服务（包括即时的和非即时的）时，能够联系沟通的方式包括：服务热线电话和联系人、联系单位信息、信函/传真、电子邮件、服务网站。

3.技术服务方式

提供多种服务方式，以便于帮助用户解决问题。

在线服务：通过网络的方式提供技术服务；

电话服务：提供技术服务电话，为用户进行技术答疑服务；

远程服务：通过远程的方式帮助用户解决问题。

## 网站管理系统功能需求（新建）

### 需求

网站平台应内置对模板文件和风格文件的内容管理功能。

应支持在站点、节点等各处设置模板的页面中直接编辑相应的模板。

应支持在站点、节点等各处设置模板时，在选择模板页面智能推荐最相关的模板文件。

应支持数据备份/还原。应支持平台级和站点级两级备份/还原。平台级的模板备份/还原可以针对整个平台的所有模板和风格文件进行备份/还原，站点级的备份/还原则是只针对当前站点的所有模板和风格文件进行备份/还原。备份包中的文件除了模板文件以外，还包含风格样式文件，包含所有设备。还原时不覆盖没有修改过的文件，以避免因为模板文件修改而引发清理全站缓存。

应支持定时自动备份和对过期备份包文件的自动清理

### 编辑器需求

编辑器应支持仿word的可视化内容编辑方式，实现所编辑内容的“所见即所得”。编辑器应支持插入图片、视频、音频、附件、表格、符号、PDF文件、百度地图、日期、时间、特殊符号、公式、分隔线等多种元素。

编辑器应支持标准、完整、简洁、极简、手机、微信等多种模式，以满足平台各功能模块在不同应用场景的调用需要。

编辑器应支持Word文档一键导入的功能，文档内容直接导入到编辑器且保留源格式和表格， 导入的Word文档格式应支持.docx、.doc、.wps（金山wps、永中office的文档格式），导入时应支持设置“将文件名/内容第一行设置为标题”、格式清理（清除格式、首行缩进、清除字号、清除字体、清除链接、清除图片）选项。

应支持从Word文档中直接粘贴内容拷贝到编辑器中时可根据情况选择是否过滤掉无关的格式代码。

应支持将截图直接粘贴到内容编辑器中即可自动上传到服务器。

应支持自动下载远程图片到服务器本地。

应支持手机扫码上传功能，手机通过扫描二维码后就可以将手机中的图片直接上传到网站中，而不需要把手机上的图片导入电脑后再通过电脑上传。

应支持多种一键排版方案，应支持一键去除文档中的无用格式代码。

应支持所见即所得的公式编辑。

编辑器中的内容应支持手动分页功能。

编辑器中的表格如果过宽或过高时，前台显示时应该只显示为预设大小并自动加上滚动条。

应支持整合错别字和敏感字检查，对于发现的每个错别字和敏感字，点击时编辑器中的内容中同步定位相应位置并标记显示，编辑人员可以人工确认，确认是错别字和敏感字时可点击“更正”按钮让系统自动更正。

应支持插入图片、视频、音频、附件时，可以直接上传。

应支持设置了不常见字体时进行闪烁提醒。

### 医患互动系统

便民咨询系统主要是用于在网站群平台上开设简单的便民咨询类的互动交流类栏目。

便民咨询系统应包含便民咨询配置、信件分类管理、信件提交与结果查询、信件处理与督办、信件评论管理、信件统计等功能子模块。

**信箱管理**

应支持站点中可以增加多个多级信箱，便于再前台开设多种不同的互动类留言和信箱。

应支持管理员可以为每个信箱指定列表页，写信页，内容页的前台模板。

应支持创建、修改、删除、搜索多级信箱。

应支持以树形列表的方式查看多级信箱分类。

应支持删除信箱后，记录信箱的删除记录到平台的删除记录。

应支持信箱进行归档操作。归档的信箱分类在前台不能再继续留言。

应支持配置所有站点默认使用的页面模板配置和写信须知内容。

**留言展示**

应支持根据信件分类展示的公开的最新留言。

应支持信件搜索。

应支持修改、查看、删除、搜索、筛选等操作。

应支持按类型、信件状态、用户公开状态、公开状态、审核状态等条件进行筛选。

### 日志管理系统需求

应支持记录、查询系统后台的操作日志，日志内容应该包括用户名、记录时间、来源、IP地址及详细信息等，并应支持excel方式导出全部系统操作日志记录。应支持操作日志定期自动清理功能。

应支持记录、查询系统后台的安全日志，日志内容应该包括用户名、记录时间、来源、IP地址及详细信息等，并应支持excel方式导出全部系统安全日志记录。

应支持记录、查询用户帐户的安全日志，日志内容应该包括用户名、记录时间、来源、IP地址及详细信息等，并应支持excel方式导出全部用户帐户安全日志记录。

应支持记录、查询用户帐户的安全防护日志，日志内容应该包括用户名、锁定时间、解锁时间、来源、IP地址及详细信息等，并应支持excel方式导出全部用户帐户安全日志记录。

应支持、查询记录系统后台的数据添加、修改、删除日志，日志内容应该包括站点名称、“修改”时间、数据类型等，并应支持excel方式导出全部系统数据删除日志记录。

▲应支持是否开启异常配置日志记录功能，开启时系统会拦截所有的服务器内部错误并将其记录到异常日志中，异常日志须以文件的形式记录到系统目录中。应支持记录、查询系统后台的系统异常日志，日志内容应该包括时间、文件大小、文件内容等，并应支持单条、批量或者直接清空系统异常日志记录。

应支持对第三方系统调用的接口信息进行记录。

## 权限及审核需求

**平台权限管理**

应具备统一权限管理能力，提供角色管理功能，实现对服务的访问控制和机构的服务授权。通过对各类操作权限、数据权限设置和组织机构设置紧密配合来实现业务分工以及业务权限管理。

角色根据权限大小分成平台角色（平台超级管理员和平台普通管理员）、站点角色（站点超级管理员和站点普通管理员）和节点角色三级。

节点角色的权限再细分成三种权限：操作权限（如查看、录入、修改、审核、管理等，审核权限能根据多级审核流程的需要再进一步在多级审核流程分配在各审核步骤中的权限）；操作数据的范围（自己的/部门的/所有人的）；字段权限（在录入修改界面中角色可以设置哪些字段的值）。通过配置各栏目（节点）节点角色的管理员即可对各栏目指派不同的管理员进行管理。

平台超级管理员可统一管理全平台所有站点的数据，可以对站点功能进行配置，并拥有管理所有子站点的权限；

站点超级管理员可修改所属站点模板，可增删改栏目、本站点的管理员、专题模板等，可配置本站点的所有管理员权限，可将权限细分下发到本单位内设机构或下属单位，实现多人管理维护子站信息；

应支持按节点批量设置权限和按管理员批量设置权限两种操作方式，按节点批量设置权限指可以批量添加或替换指定节点的各节点角色的管理员，按管理员批量设置权限指可以批量添加或替换指定管理员在各节点中的节点角色。

互联网用户则以用户组的方式进行权限分配，可以配置用户组的前台访问权限、投稿权限等。

**管理员管理**

应支持创建、修改、查看、删除、搜索、筛选、锁定、解锁、重置密码、重置错误登录次数、查看权限、批量删除、批量锁定、批量解锁、批量重置密码等常用功能；

应支持按登录次数、最后登录时间、是否锁定、是否已经填写手机号码等条件进行筛选；

**内容审核节点管理**

应支持超级管理员、站点角色、节点角色对内容的审核权限，内容信息员发布信息后，短信通知到相应的管理员审核，支持三审三核，每一个角色可以查看内容的审核节点具体到那一步（审核流程图），并支持显示查看每一步审核用时时长。

#  项目实施进度

## 总体进度要求

说明：对项目建设的总体时间节点进行描述。

系统自项目批复启动之日起3个月完成建设，上线使用。

## 分阶段实施进度要求

项目分为几个关键里程碑并标明完成时间。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **阶段** | **名称** | **建设目标** | **工作内容** | **产出物** | **工期进度** |
| 第一阶段 | 项目策划 | 项目策划、组间协调、计划与跟踪 | 项目准备、项目估算、实施计划、协调、计划分解 | 总体设计方案项目实施计划项目实施计划变更协议 | 1天 |
| 第二阶段 | 网站风格、栏目规划及功能需求调研 | 信息资源梳理、策划、网页风格及栏目规划 | 针对网站风格、栏目、功能进行细化，形成初步设计稿 | 设计稿需求规格说明书需求确认报告 | 4天 |
| 第三阶段 | 网站设计稿确认与修改 | 页面设计确认及修改 | 确认需求及页面设计。美工负责设计、调研及与客户进行确认、沟通、修改、确认。 | 页面设计确认单 | 10天 |
| 第四阶段 | 网站的实施及数据迁移 | 网站页面以及功能构建，迁移原有网站的数据 | 功能构建、美工设计、页面实施，对原有网站的数据进行迁移。 | / | 7天 |
| 第五阶段 | 测试调整 | 完成系统运行和数据完整测试 | 对实施完成的系统、网站进行测试，测试网站功能是否正常，内容是否完整 | 测试报告系统试运行阶段用户问题反馈确认单 | 3天 |
| 第六阶段 | 培训 | 对系统操作使用人员进行培训 | 对系统操作使用人员进行培训 | 用户培训计划表用户培训记录表用户培训文档系统安装维护手册用户操作手册系统管理员手册…… | 1天 |
| 第七阶段 | 交付和验收 | 验收测试、试运行和交付使用 | 开发文档的收集整理、项目工程打包、验收测试书面报告安全性检测，安全检测报告。 | 系统验收报告项目总结报告信息系统安全测评报告 | 2天 |
| 合计： | 28天 |