**乌恰县人民医院OA系统办公自动化采购软硬件清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **个人事务** | | | | |
| * **电子邮件** | | 主要用于内部、外部用户邮件的收发。（支持pop3邮件收发，支持和内部邮箱的集成。可以从内部邮箱直接发送到外部邮箱。） | | |
| * **消息管理** | | 主要起通知、提醒和交流作用。 | | |
| * **公告通知** | | 主要具有通知公告的发布、管理和查询等功能 | | |
| * **新 闻** | | 主要新闻发布、新闻评论、管理和查询功能。 | | |
| * **投 票** | | 主要用于意见收集、民主决策、结果测试等。 | | |
| * **个人考勤** | | 主要用于对单位内部员工考勤的管理。 | | |
| * **日程安排** | | 主要是对未来要做的事务进行安排。 | | |
| * **工作日志** | | 主要是对已经做的工作进行记录。 | | |
| * **通 讯 薄** | | 主要是对联系人信息提供分组、按姓氏索引，导入导出等功能。 | | |
| * **个人文件柜** | | 主要用来存放用户自有文件。 | | |
| * **控制面板** | | 主要是对包括界面主题、快捷菜单组、个人资料等11个组块进行适合单位或个人的个性化设定。 | | |
| **工作流程审批** | | | | |
| * **新建工作** | | 主要是对用户有新建权限的所有工作流程以及相应的分类工作的开展。 | | |
| * **我的工作** | | 主要是未接收、待办理、办理中、已完结、挂起的工作状态的体现、提醒。 | | |
| * **工作查询** | | 主要有按制定的条件进行工作查询与按流程等工作字段进行查询；查询后可导出word文档、html文件。 | | |
| * **工作监控** | | 主要对某个流程的工作办理情况的监控、管理（工作进行转交、委托等操作）。 | | |
| * **数据报表** | | 主要是可根据管理员自主设计，主动生成数据报表，助用户单位进行合理化数据分析的作用。 | | |
| * **超时统计分析** | | 主要是对工作中出现的超时进行查询及备案，并可对超时工作进行统计（html列表显示，导出CSV进行柱状图分析）。 | | |
| * **工作委托** | | 主要对工作进行委托，可设置委托内容及时间段，并可查看个人的委托与被委托记录。 | | |
| * **工作销毁** | | 主要是一个回收站的作用，对已删除的工作可进行恢复，和彻底销毁。 | | |
| * **流程日志**   **查询** | | 主要是对指定条件下的工作所有办理流程进行查询（包括办理、转交及回退的操作），可以了解流程个步骤的办理情况。 | | |
| * **数据归档** | | 主要是对选择日期前的数据进行归档，方便对数据的查询，同时优化系统性能，提高速度。 | | |
| **行政办公** | | | | |
| * **公告通知管理** | | 具有通知公告的发布、管理和查询等功能 | | |
| * **公告通知审批** | | 当发布公告通知设置为需要审批时，公告通知的发布就需要经过审批程序。 | | |
| * **新闻管理** | | 新闻发布、新闻评论、管理和查询功能 | | |
| * **投票管理** | | 主要用于意见收集、民主决策、结果测试等 | | |
| * **日程安排查询** | | 主要是对未来要做的事务进行安排查询 | | |
| * **工作日志查询** | | 主要是对已经做的工作进行查询 | | |
| * **工作计划** | | 多人参与，参与人随时可以看到任务进度，相关人可以批示。 | | |
| * **办公用品管理** | | 用于单位办公用品、低值易耗品的日常管理。 | | |
| * **固定资产管理** | | 实现固定资产的录入，生成资产卡片，生成相应的查询报表。 | | |
| * **图书管理** | | 实现图书的管理录入、借阅、查询、管理。 | | |
| * **资源管理** | | 对单位可以借出设备的管理，比如笔记本电脑、投仪影等。 | | |
| * **会议管理** | | 对单位的会议室、设备、会议的申请与批准等进行全面管理。 | | |
| * **车辆管理** | | 主要实现对单位的车辆信息、维护等进行全面管理。 | | |
| **知识管理** | | | | |
| * **公共文件柜** | | 主要用来管理部门或单位的文件。 | | |
| * **网络硬盘** | | 存放资源文件、管理资源文件，比如杀毒软件、驱动等。 | | |
| * **图片浏览** | | 主要用于放JPG、GIF等图片格式文件，可以直接播放。 | | |
| * **OA知道** | | 先建立好词条，在知道的首页上，可以直接在搜索栏输入问题，点击搜索，就会出现多条已解决的相关问题与答案。 | | |
| * **维基百科** | | 维基知识库所提供的，是一个企业内部所有用户均能平等的浏览、创造、完善内容的平台。 | | |
| * **文档检索中心** | | 全文检索系统需要具有建立索引。处理查询返回结果集，增加索引，优化索引结构等功能。 | | |
| **人力资源** | | | | |
| **人事管理** | | 人事档案 | 实现在职人员和离职人员基本信息的管理、查询，包含三个菜单项：人事档案管理、人事档案查询和统计分析。 | |
| 档案查询 | 可以查看管理范围内的用户的档案信息。 | |
| 合同管理 | 针对与员工相关的合同进行管理，如试用期合同、劳动合同、保密合同等。 | |
| 奖惩管理 | 针对员工的日常工作表现，根据单位制度所作出的对员工的奖励、惩罚。 | |
| 证照管理 | 用于管理员工的一些职业证照信息、归于某人管理的单位证照信息、证照的电子副本。并且可以设置提醒日期，到时自动提醒。 | |
| 学习经历 | 用于管理员工学习经历情况，同时可以记录在学习过程中的表现，如获奖情况、证书情况。 | |
| 工作经历 | 用于管理员工以前的、现在的工作单位，在该单位的表现情况等信息。 | |
| 劳动技能 | 用于管理员工的特长、所掌握的技术、所拥有的技能。并且记录下发证机关、技能证书单子副本等信息。 | |
| 社会关系 | 用于管理员工的亲友信息，包括职业及联系方式等。 | |
| 人事调动 | 人事调动用于管理员工调动情况，包括职务、单位、部门的变动情况。 | |
| 离职管理 | 用于管理员工的离职情况，记录离职时间，去向及离职前的工作交接情况。 | |
| 复职管理 | 用于记录以前离职员工的复职情况，复职操作后，自动恢复到复职的部门中。 | |
| 职称评定 | 用于管理员工的职称评定信息。包括所获职称、评定时间等。 | |
| 员工关怀 | 用于对员工的关怀记录，关怀内容可以是生日礼物、节日礼品、员工活动等，带有关怀提醒功能，自动显示当月过生日的员工。 | |
| 人事分析 | 用于对人事管理下各个模块，进行统计分析，以辅助人力资源管理员及单位领导进行人事决策与人事调整。 | |
| **招聘管理** | | 招聘需求 | 用于单位各部门主管向人力资源管理员提交用人需求 | |
| 招聘计划 | 各部门提交来的人才需求，制定一段时期单位的招聘计划，主管领导同意后，实施招聘。 | |
| 人才库 | 收集整理合适的招聘人选，将其简历录入人才库。 | |
| 招聘筛选 | 针对收集的简历信息，选出需要进行面试或笔试的简历 | |
| 招聘录用 | 对招聘通过的应聘人员进行录用，并设置好正式入职时间和起薪时间。 | |
| 人才分析 | 对人才库中的简历信息，人才分析模块可以按照多种统计条件对信息进行图形化统计分析。 | |
| **培训管理** | | 培训计划 | 可以针对单位的业务发展情况，制定相应的培训计划。 | |
| 培训记录 | 针对培训结果，给予参与培训的员工，进行培训记录，包含培训评估和培训  费用。 | |
| **考勤管理** | | 考勤审批 | 可以对单位的外出，请假，加班情况进行审批处理。 | |
| 考勤记录 | 可以查看单位某人的考勤记录。 | |
| 考勤统计 | 可以查看某一部门或所有部门一段时间内的考勤情况，并且可以统计出excel等格式的文档。 | |
| 值班排版管理 | 用于管理单位值班的安排，值班日志、值班记录查询和导出。 | |
| 查岗质询登记 | 用于管理单位的值班缺岗情况进行记录和说明。 | |
| **绩效管理** | | 可以实现对单位员工的各种简单考核如季考核、月考核等。考核完毕之后，可以看到考核结果，也可以将结果导出为EXCEL文件和汇总文件。并且员工可以参与考核自评。 | | |
| **积分管理** | | 通过积分管理来全面反映员工的工作表现，OA中工作办理情况，员工个人素质。如果积分与员工待遇挂钩，有助于调动员工工作积极性、主动性，也有助于单位管理。 | | |
| **薪酬管理** | | 主要实现工资的录入、上报管理及工资审核管理工作。工资流程管理、财务工资录入和部门工资上报。利用工资管理模块，财务人员可以定义工资项目，新建工资上报流程查看各部门工资上报的报表等。 | | |
| **在线考试** | | 可以设置题库、设置试题，进行灵活的试题抽取，组织各种网络在线考试、竞赛等。 | | |
| **档案管理** | | | | |
| **档案管理** | | 卷库管理 | 针对企业文件档案管理需求而设计。可以指定卷库所属部门 | |
| 案卷管理 | 填上案卷的相应属性，选择所建案卷所属卷库。 | |
| 文件管理 | 可以建立具体档案文件，并且将文件归入相应的案卷中， | |
| 案卷借阅 | 包含借阅申请和借阅审批两个模块，在借阅申请中查看相应案卷中的文件，可以申请借阅。 | |
| 档案统计 | 包含借阅统计和案卷统计两个模块，借阅统计是对文件的借阅次数进行统计；案卷统计是对案卷中的文件个数进行统计。 | |
| 档案销毁。 | 档案销毁是对文件管理中销毁的文件彻底删除。 | |
| **项目管理** | | | | |
| **项目管理** | | 我的项目 | 新建项目，可以根据类型和时间进行查询 | |
| 我的任务 | 显示近期工作的信息、描述、任务周期和工时 | |
| 项目审批 | 领导对项目可以进行审批，并可以查看审批记录 | |
| 项目文档 | 对项目中的文件进行管理，可以设置不用的权限 | |
| 智能报表系统 | | | | |
| 智能报表是一款以管理表格为模型构建企业数据管理及统计分析的工具型软件，它融合电子表格和数据库软件的优势，有类似电子表格展示形式灵活多样和操作简洁高效的特点，同时又有数据库软件便于大规模存储和统计分析的特性。  智能报表集系统设计和系统运行于一体，用户无需掌握编程语言即可轻松构建适宜单位自身需要的个性化管理信息系统，比如费用报销系统等涉及管理的各个方面。 | | | | |
| 系统集成 | | | | |
| 1、数据：  集成协同办公平台待办事项，组织自动同步更新，通过移动app登录访问办公平台，实现待办推送，即时将消息推送到桌面。  2、HIS门诊量统计数据：  抓取HIS系统相关数据，实现办公平台及手机移动端的查询和查看。  3、HIS住院量统计数据  抓取HIS系统相关数据，实现办公平台及手机移动端的查询和查看。  4、HIS全院病人费用统计数据：  抓取HIS系统相关数据，实现协同办公平台及手机移动端的查询和查看。  5、其他医院要求的HIS数据：  抓取其他医院要求HIS系统相关数据，实现协同办公平台及手机移动端的查询和查看 | | | | |
| 配套硬件服务器 | | | | |
| 服务器 | 8核cpu、12G内存、1T硬盘、双网卡及以上配置 | | | 1台 |

## 第二代防火墙

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| **配置要求** | 整机吞吐量≥6Gbps；应用层吞吐量≥800Mbps；并发连接数≥1, 800,000；每秒新建连接数≥6万；标准1U机架设备,标配4个千兆电口，2个千兆光口，并含2个高速USB2.0接口，1个RJ45串口；硬盘≥500GB；标准1U架构。 |
| **部署方式** | 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式。 |
| **路由支持** | 支持静态路由，ECMP等价路由。  支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议。  支持多播/组播路由协议。  支持路由异常告警功能。  支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能。（提供产品界面截图） |
| **基础功能** | 访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式。  支持根据国家/地区来进行地域访问控制。（提供产品界面截图）。  能够识别管控的应用类型超过1200种，应用识别规则总数超过3000条。  支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制。 |
| **DoS/DDoS攻击防护** | 支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护，支持SYN Flood、IPv4和IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测。 |
| **入侵防护功能** | 设备具备独立的入侵防护漏洞规则特征库，特征总数在7000条以上。 （提供产品界面截图）  支持对服务器和客户端的漏洞攻击防护。  支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。  具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能。  可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则。（提供产品界面截图） |
| **Web应用安全防护** | 设备具备独立的WEB应用防护识别库，特征总数在3500条以上； （提供产品界面截图）  支持抵御SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB整站系统漏洞等攻击；（提供产品界面截图）；  为满足等级保护要求中漏洞管理要求，需要配套提供漏洞管理工具，能够对操作系统和Web漏洞进行检测；（提供产品界面截图）  支持对网站黑链进行检测；  要求配套提供10套网页防篡改软件，并能够与设备进行联动阻断篡改攻击；（提供产品界面截图）  为实现管理员对高级威胁的快速响应，要求支持高级威胁关联分析的能力，并展示热点事件详情，推送到运维管理员手机中进行快速处置； |
| **僵尸主机检测** | 设备具备独立的僵尸网络识别库，特征总数在58万条以上。（提供产品界面截图）  支持DNS代理场景下重定向恶意域名。  支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。  对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告。 |
| **终端联动响应** | 配套提供10个终端安全监测与响应组件，能够对终端安全进行病毒查杀、终端微隔离等。  支持与终端安全管理平台的联动，实现管理员在第二代防火墙平台通过终端安全管理平台对其下属终端下发快速查杀任务、并根据查杀结果并进行处置； |
| **安全可视化** | 支持业务安全和用户安全的风险展示。  支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别。  支持在同一个界面对全网所有服务器和主机的威胁进行风险评估，支持对当前所有业务的安全防护状态进行动态保护，支持对所有已被入侵和受控的设备进行风险检测与分析，针对风险可以实现快速响应与处置。上述整个流程从风险评估到动态保护，检测与分析，响应处置可提供管理员一键评估，自动化展示最终的风险（提供产品界面截图）  支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证。 |

## 日志审计

|  |  |
| --- | --- |
| **项目** | **功能指标要求** |
| **基本要求** | 采用标准机架式硬件。审计主机至少提供千兆RJ45\*6（一路数据传输口。一路系统管理口）。网络接口支持电口，可升级为光口。所供系统设备必须自带本地存储功能。可用物理磁盘空间>=1TB。日志存储量至少十亿条。日志采集能力：3000条/秒以上。支持后期扩展外部网络存储(IP SAN、NAS、DAS、磁盘阵列等)。内置50个主机审计许可证书。 |
| **数据采集** | 支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]、AS400日志、数据库访问[Mysql]、WEB访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]、FTP服务[VSftpd、NCftpd、Proftpd、Glftpd、Serv-u]。  支持SNMP日志采集，支持日志类型：网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]  支持Opsec Lea日志采集。  支持镜像数据采集，支持类型：数据库模块[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览、论坛微博]、入侵检测、业务检测、流量监控。  支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储。（提供产品页面截图证明）  支持文本型日志原始文件管理，可将系统作为日志服务器使用。（提供产品页面截图证明） |
| **监控功能** | 支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况。支持自定义配置实时监控的日志类型。支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警。支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况。支持实时监控系统当前运行状态，包括系统CPU、内存、硬盘状态及管理员操作。 |
| **查询分析功能** | 支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索。（提供产品页面截图证明）  支持按日志文件的名称、内容进行检索，并提供页面下载原始日志文件。支持查询模版创建、修改、删除功能。（提供产品页面截图证明） |
| **策略管理功能** | 支持内置归并策略，对HTTP数据进行自动归并处理。（提供产品页面截图证明）支持内置关联分析策略，可设定用户在规定时间内连续多次输入错误口令产生告警或事件。  支持数据策略，可设定采集多种WEB访问数据，包括：脚本访问、样式访问、图片访问及地理数据访问。  支持自定义创建实时审计规则：根据日志字段为条件预设置分析策略。  规则条件设定支持逻辑运算符与支持正则表达式。（提供产品页面截图证明）  支持自定义三层业务策略：支持通过该策略配置，识别数据库三层架构中用户信息。 |
| **数据管理功能** | 支持按日志属性、日志类型、时间范围进行数据备份。。支持WEB界面备份及日志恢复导入工作。支持自动与手动两种备份归档方式。  系统支持以FTP上传方式将归档文件存储到第三方存储系统中。（提供产品页面截图证明） |
| **日志权限** | 审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明。（提供产品页面截图证明）支持日志类型、IP地址权限设置。支持页面功能模块权限设置。 |

防病毒系统

|  |  |  |
| --- | --- | --- |
|  | 序号 | 详细参数 |
| **部署 管理** | 1 | 须提供文件特征云查询服务器，云查询服务器能够连接厂家共有安全云系统自动进行文件特征查询同步，且能够支持隔离网环境。 |
| 2 | 多样式的帐户管理设置，默认可分配三种管理员权限，普通管理员、配置管理员、审计管理员，并可以按实际需求，手动修改具体权限，可适应企业不同人员权限的划分设置，以保证灵活与安全管理规范。 |
| 3 | 自主授权分割功能，管理员可以从主系统中心分割授权客户机数量给下级系统中心，限制下级系统中心对客户机的注册数量，阻止非法客户机注册。 |
| 4 | 须提供全网集中漏洞扫描及修复技术（包括隔离网络解决方案），提供网络内客户机存在漏洞补丁汇总报告，远程完成系统补丁程序的安装，以解决网内系统的漏洞修复问题。修补过程勿须客户机参与，客户机以非管理员权限登录，也能完成漏洞扫描和修复。 |
| 5 | 系统中心控制台具有消息推送功能，能够实现网络管理人员对全网或者指定客户机发送消息 |
| 6 | 提供客户端边界管理功能，对通过优盘、网络共享、互联网、下载工具邮件以及QQ类通讯软件进入的文件给于安全性鉴定，能够向用户报告这些文件是否为安全文件，有助于帮助终端用户在确认为安全文件时再执行，并且具备溯源功能，对于鉴定为未知的文件则谨慎处理。（须提供产品功能截图） |
| 7 | 支持与动态行为分析系统的联动。（须提供产品功能截图） |
| 8 | 须实现与防毒墙等网关类安全设备联动，形成关与端的联动防御体系，并在防病毒软件控制台展示出协议层病毒和恶意通讯等防毒墙拦截数据。（须提供产品功能截图） |
| **客户端功能** | 1 | 要求占用系统资源低，网络版杀毒软件的客户端程序在监控状态占用系统资源CPU不高于10%，内存占用不超过30MB |
| 2 | 产品终端程序须集成宏病毒专杀模块，并可在未安装office软件时也能对宏病毒进行查杀 |
| 3 | 具备系统优化功能，能够统计开机时间，对开机所加载的启动项进行管理，可以关闭无需开机就加载的项目，提升开机速度；能够对启动项、系统服务项、计划任务项以及应用程序的扩展加载项进行开启或关闭处理。 |
| 4 | 客户端需支持“虚拟环境轻客户端模式”，安装在虚拟机上的“轻终端”将快速响应调度器的统一指令，使得服务器整体时时刻刻保持很低的负载，从而将其对机器性能的影响降到最低。虚拟化终端需同时支持多个虚拟化系统，如VMware、Microsoft Hyper-V和华为平台等。 |
| 5 | 客户端须支持至少包括麒麟、红旗、红帽操作系统在内的国产操作系统。 |
| **服务器端** | 1 | 针对Windwos Server操作系统进行病毒查杀，提供主动防御系统防护,补丁管理功能，支持对全网终端系统漏洞发现、补丁智能修复、强制修复等、蓝屏修复、补丁分发流量控制、客户端P2P补丁分发加速等功能。系统默认支持WIN2003/WIN2008/WIN2012/，含三年升级服务。 |

**交换机**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **交**  **换**  **机** | 24口交换机 | 24个10/100/1000Base-T 以太网端口，4个千兆SFP  交流供电,包转发率：51Mpps/126Mpps,交换容量：336Gbps/3.36Tbps | 3 | 台 |  |
| 48口交换机 | 48个10/100/1000Base-T 以太网端口，4个万兆SFP交流供电,包转发率：87Mpps/144Mpps,交换容量：336Gbps/3.36Tbps | 2 | 台 |  |

## 等级保护测评参数

一、**项目服务范围**

本项目将对2个信息系统进行进行测评。

重要信息系统的名称和数量如下表所示。

| 序号 | 信息系统项目名称 | 系统等级 |
| --- | --- | --- |
| 1 | 乌恰县人民医院HIS系统 | 二 |
| 2 | 乌恰县人民医院电子病历系统 | 二 |

**二、项目服务内容**

|  |  |
| --- | --- |
| 工作阶段 | 具体内容 |
| 安全整改  方案设计 | 安全管理设计：根据《信息系统等级保护测评报告》，对信息安全保障中各种制度、规章以及相关制度规章的落实，进行细致的规划设计； 安全技术设计：根据《信息系统等级保护测评报告》，从物理安全、网络安全、主机安全、应用安全、数据安全五个方面，对机房物理环境、网络结构、策略配置、工具评估结果等详细分析，根据分析结果设计安全技术方案，通过对现状的设计规划，完成《信息系统安全整改建设方案》。 |
| 等级测评 | 由测评机构开展等级测评工作。包含现场正式测评工作、渗透测试、配置审计、远程扫描等，并出具《信息系统安全等级测评报告》。 |
| 测评范围：物理环境、网络设备、安全设备、服务器、终端、数据库、业务系统、安全管理机构、人员安全管理、安全管理制度、系统建设、系统运维。 |
| 工具测试：通过工具扫描测评范围内的系统及网络，进行渗透测试、安全配置审计、脆弱性扫描，发现安全风险、漏洞和威胁。 |
| 人工检查：机房物理设施、网络设备、安全设备、服务器、终端、业务系统的安全策略及其日志分析。 |
| 网络构架分析：网络安全规划、设备命名规范性、网络架构安全性。网络设备和链路冗余、设备选型及可扩展性。网络设备的ACL、防火墙SNMP、口令、设备版本、系统漏洞、服务、端口等。 |
| 问卷调查：对管理人员、维护人员、业务人员进行问卷调查，问卷涉及威胁与管理脆弱性两个方面。 |
| 应用系统调研：通过人工安全检查了解目前应用系统本身的安全性内容，了解前期信息安全建设中的安全思想是否能够准确的表达与使用。 |
| 顾问访谈：了解各个层次的人员，了解目前网络中技术的缺陷、管理体系的缺陷。对制度的执行情况进行更为细致的了解和评定。 |
| 安全培训 | 网络安全知识培训、信息安全等级保护技术培训、网络攻防技术培训。 |

依据国家相关信息安全标准和规范，严格遵循《信息安全技术信息系统安全等级保护测评要求》和《信息安全技术信息系统安全等级保护测评过程指南》文件，根据本项目信息系统已完成的定级备案安全等级，开展相应级别的安全等级测评工作，测评工作包括技术测评和管理测评两部分，分别为：

**1、技术测评**

1.1物理安全：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护。

1.2网络安全：网络安全测评通过访谈、检查和测试的方式评测信息系统的网络安全保障情况。主要涉及对象为信息系统的网络拓扑结构、网络设备以及网络安全设备等三大类，具体的测评内容如下所示：结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护。

1.3主机安全：主机系统安全测评通过访谈、检查和测试的方式，测评信息系统主要服务器操作系统和主要数据库管理系统安全保障情况。具体测评内容包括：身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制。

1.4应用安全：应用安全测评通过访谈、检查和测试的方式评测生产系统的应用安全保障情况。主要涉及的对象为应用软件系统，具体测评内容包括：身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制。

1.5数据安全：数据安全测评通过访谈和检查的方式评估生产系统的数据安全保障情况。重点检测信息系统的数据在采集、传输、处理和存储过程中的安全，以及数据备份恢复的安全。具体测评内容包括：数据完整性、数据保密性、备份和恢复。

**2管理测评**

2.1安全管理制度：安全管理制度测评通过访谈和检查的形式评估安全管理制度的制定、发布、评审和修订等情况。主要涉及的对象为安全主管人员、安全管理人员、其他人员、管理制度、操作规程文件等，具体测评内容包括：管理制度、制定和发布、评审和修订。

2.2安全管理机构：安全管理机构测评通过访谈和检查的形式评估安全管理机构的组成情况和机构工作组织情况。主要涉及的对象为安全主管人员、安全管理人员、相关的文件资料和工作记录等，具体测评内容包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

2.3人员安全管理：人员安全管理测评通过访谈和检查的形式评估机构人员安全控制方面的情况。主要涉及对象为安全主管人员、人事管理人员、相关管理制度、相关工作记录等，具体测评内容包括：人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理。

2.4系统建设管理：系统建设管理测评通过访谈和检查的形式评估系统建设管理过程中的安全控制情况。主要涉及对象为安全主管人员、系统建设负责人、管理制度、操作规程文件、执行过程记录等，具体测评内容包括：系统定级、安全方案设计、采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、安全服务商选择。

2.5系统运维管理：通过访谈和检查的形式评测系统运维管理过程中的安全控制情况。主要涉及人员有安全主管人员、安全管理人员、运维人员，涉及内容有运维管理制度、运维服务团队的管理制度、操作规程文件、执行过程记录等。具体测评内容包括：环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理。

根据以上10个层面的现场测评结果出具相应的单项和整体测评报告，测评报告需得到项目单位的确认，并报请省公安厅主管部门审核、批复。测评报告编制的内容及格式严格遵照《信息安全等级保护测评报告模版（2015年版）》公信安[2014]2866号进行。

**3等级保护测评培训**

3.1测评机构必须提供本项目所需的现场培训。

3.2培训目的：使招标人人员熟悉国家对信息安全等级保护相应法律法规；使甲方人员熟悉信息安全等级保护测评的方法。

3.3培训内容：信息安全等级保护法律法规；信息安全等级保护测评方法。

3.4培训对象：招标人信息系统使用及安全管理人员。

3.5培训教师：培训教师须具备相关专业认证资质与丰富经验。

3.6培训人数：现场培训人数根据甲方需求确定。

3.7培训天数：根据招标人需求确定。