合同编号:_____

# 郑州大学

# （郑州大学继续教育学院远程教育学院支撑平台运维管理系统）

# 采购合同

甲方： 郑州大学

乙方： 河南丰联信息科技有限公司

## 一、 合同内容及要求

1、合同内容

郑州大学继续教育学院远程教育学院支撑平台运维管理系统（具体内容详见附件一技术参数要求）

2、合同要求

甲乙双方在签订合同的同时，签订《郑州大学信息系统建设网络安全责任协议》和《郑州大学信息系统建设信息安全保密协议》。

## 二、合同总价款

本合同总价款为人民币（大写）贰拾陆万玖仟 圆整（￥269000 元）。

| 序号 | 产品名称 | 单价（元） | 数量 | 合计（元） | 交货期 |
|---|---|---|---|---|---|
| 1 | 支撑平台运维管理系统（丰联定制） | ¥239,700.00 | 1 | ¥239,700.00 | 30 日历天 |
| 2 | 数据处理工作站(联想 IdeaCentre GeekPro) | ¥16,000.00 | 1 | ¥16,000.00 | 30 日历天 |
| 3 | 显示器（小米 RMMNT238NFS） | ¥900.00 | 8 | ¥7,200.00 | 30 日历天 |
| 4 | Wifi6 路由器（华三 NX54） | ¥500.00 | 1 | ¥500.00 | 30 日历天 |

| | | | | | |
|---|---|---|---|---|---|
| 5 | 办公椅（京东京造 Z9 SMART） | ¥700.00 | 8 | ¥5，600.00 | 30 日历天 |
| 总计 | | 人民币 贰拾陆万玖仟 圆整（￥ 269000 元） | | | |

**三、质量要求或服务标准，乙方对质量负责的条件和期限**

按照“附件二：项目其他要求”所属的内容和标准提供满足要求的高质量服务，在签订合同后 30 个日历天完成项目交付，并对交付项目提供三年质保。

**四、服务约定**

1、 交货时间： 合同签订后 30 个日历天 。

2、 交货地点： 甲方指定地点 。

3、 交货方式： 甲方指定方式 。

**五、验收标准、方法**

1、 软件产品已经完整的部署在甲方提供的指定服务器资源上，配置学校内网测试 IP 地址，使用安全合规的测试数据，并在此运行环境上进行信息系统的功能测试、性能测试、安全测试等工作。

2、 功能测试。乙方提交软件产品的功能测试报告，并对功能测试报告的真实性承担责任。乙方依据软件产品开发需求、设计文档、采购时的技术参数要求并结合功能测试用例等完成软件产品的功能测试，形成功能测试报告。

3、 性能测试。乙方提交软件产品的性能测试报告，并对性能测试报告的真实性承担责任。乙方依据软件产品开发需求、设计文档、采购时的技术参数要求，在用户量、数据量的超负荷下，对软件运行时的相关数据进行分析测试，形成性能测试报告。

4、 代码安全审计。乙方提交软件产品完整的、真实的、功能一致的源代码进行代码安全审计。如因特殊原因无法提供源代码的，由乙方委托具有中国计量认证（CMA)或中国合格评定国家委员会（CNAS)认可实验室证书等资质的第三方软件代码测评机构出具的代码审计合格报告。报告中的软件源代码要和实际部署的软件产品完全一致。

5、 安全风险评估。（1）乙方提交委托具有中国信息安全测评中心颁发的信息安全服务资质（风险评估类）或中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质的第三方测评机构出具的渗透测试报告；（2）乙方提交由甲方网络管理中心出具的安全基线配置核查报告和系统漏洞扫描报告。

6、 其他验收文档。乙方提交软件产品包括需求分析文档、系统设计文档、接口技术文档、数据字典文档、部署配置文档、运行维护文档和用户使用指南等相关验收资料。

**六、结算方式及期限**

根据本项目的具体情况，经甲乙双方协商后，结算费用按照阶段进行相应的比例支付，

具体如下：

1. 定制软件结算方式及期限

(1) 乙方完成合同规定的硬件设备调试后，甲方向乙方支付合同总价款的50%，即人民币（大写）拾叁万肆仟伍佰 圆整（￥134500）。

(2) 乙方完成项目的全部实施工作，且满足项目验收标准，甲方组织项目验收合格并经审计后，甲方向乙方支付合同总价款的50%，即人民币（大写）拾叁万肆仟伍佰圆整（￥134500）。

**七、免费质保约定**

项目验收通过后，免费质保3年。

**八、售后服务承诺**（包括服务的内容、方式、响应的时间、电话、质保期满结束后的维保等相关内容）

1、服务内容

1) 乙方承诺提供原厂商 三 年（不少于三年）的免费质保。质保期自项目验收合格之日起开始计算。

2) 乙方承诺在质保期内免费提供产品的运维、优化、升级以及非模块级的功能需求变更、部署结构变化等服务。

3) 乙方承诺对于本项目中存在的Bug、缺陷、安全风险隐患等，在质保期内外均提供持续的修补和消除服务。

4) 乙方承诺根据甲方所有业务系统的需求和运作规律，有针对性地制定项目系统平台的运维和售后服务保障方案，建立完善的售后服务体系。

5) 乙方承诺在售后服务过程中提供完善的文档记录，包括故障处理报告、健康巡检报告、系统性能检测调优报告、系统安全检测报告、服务年度报告等。

6) 乙方承诺提供故障分级响应机制，按照售后服务计划和质量保证承诺向甲方提供优质的技术支持服务。

2、响应方式和响应时间

| 故障级别 | 响应时间 | 技术人员到场时间 | 解决时间 |
|---|---|---|---|
| I级：属于紧急问题；其具体现象为：系统崩溃导致业务停止、数据丢失、网络安全事件和安全隐患。 | 7*24小时实时响应 | 2小时内到达现场 | 3小时 |
| II级：属于严重问题；其具体现象为：出现部分部件失效、系统性能下降但能正常运行，不影响正常业务运作。 | 7*24小时实时响应 | 2小时内到达现场 | 8小时 |

| | | | |
|---|---|---|---|
| III 级：属于较严重问题；其具体现象为：出现系统报错或警告，但系统能继续运行且性能不受影响。 | 7*24 小时实时响应 | 2 小时内到达现场 | 12 小时 |
| IV 级：属于普通问题；其具体现象为：系统技术功能、安装或配置咨询，或其他显然不影响业务的预约服务。 | 7*24 小时实时响应 | 2 小时内到达现场 | 即时 |

3、响应电话：

梁亚伟　13581791630

4、质保期外服务：

不涉及

**九、履约担保**

乙方向甲方以转账方式提供合同总价款 5%的履约保证金。履约保证金在签订合同前交学校财务处，项目验收合格、正式交付使用后予以退还。

**十、违约责任**

1、乙方违约：乙方提供的服务内容不符合约定的质量要求，甲方有权解除或终止合同，并要求乙方按合同总价款的 5%支付违约金，给甲方造成经济损失的，乙方还应如数赔偿；乙方未按约定期限交付投标物，每迟延一天须按合同总价款的 1%向甲方支付违约金。因为乙方原因造成合同迟延履行的，甲方有权解除或终止，并且要求乙方赔偿由此造成的经济损失。

2、甲方违约：甲方未能按双方约定的方式和期限支付货款，按有关法律规定对乙方承担违约责任。

3、双方其他违约责任按《中华人民共和国民法典》的有关规定处理。

**十一、争议解决**

双方在执行合同时产生纠纷，协商解决；协商不成，向甲方所在地人民法院提起诉讼。

法律文书寄送地址（乙方）：

**十二、其它约定事项：**

**十三、本合同未尽事宜经双方协商可另订补充协议。**

**十四、本合同正本十份，发包人执四份，承包人执四份，报送招标代理机构二份。**

**十五、本合同自甲乙双方签字并盖章之日起生效，随合同履行完成而自行终止。**

甲方（盖章）：郑州大学

法定代表人或代理人：

单位地址：郑州市高新区科学大道 100 号

电话：67763223

开户银行：工商银行郑州中苑名都支行

户名：郑州大学

账号：1702021109014403854

签订日期：2023.1.4

签约地点：郑州大学

乙方（盖章）：河南丰联信息科技有限公司

法定代表或代理人：梁亚伟

单位地址：河南自贸试验区郑州片区（经开）第六大街航海东路 1356 号创业中心大厦 505 室

电话： 13581791630

开户银行：招商银行股份有限公司郑州经开区支行

户名：河南丰联信息科技有限公司

账号： 371908385310801

签订日期：2023、1、3

# 附件一：项目技术参数要求

随着郑州大学继续教育学院远程教育学院信息系统建设的完善及信息系统运维管理制度的规范，建设支撑平台运维管理系统以进一步落实运维管理细则，强化系统运维，提升系统资源利用率，提高系统运维管理效率。以运维管理系统为基础，充分利用系统资源，规范运维流程，实现对运维工作的实时监控和级联展现。采用先进成熟的技术，结合学校及学院系统运维管理规定，开发运维管理系统以满足学院运维系统管理需求，在安全高效的同时满足业务需求及发展变化的需要，以保证业务系统的正常运行，感知业务系统的健康状况，在事后能够对问题进行追溯和复盘。严格按照经济、实用的原则，尽量充分利用现有资源，在系统资源预警发生后保证成本较少的申请资源分配及资源共享。

系统监控流程：采集——存储——分析——展示——报警——处理。采集信息持久化到数据库中，对集群的性能进行多维度分析、展示，以便用户能对集群进行调优或问题排查等。核心采集指标包括：cpu 使用率、cpu 温度、内存使用率、磁盘容量、磁盘 IO、硬盘 SMART 健康状态、系统负载、连接数量、网卡流量、硬件系统信息等。支持监测服务器上的进程应用、文件防篡改、端口、日志、DOCKER 容器、数据库、数据表等资源；支持监测服务接口 API、数通设备（如交换机、路由器、打印机）等；自动生成网络拓扑图，大屏可视化，web SSH（堡垒机），统计分析图表，指令下发批量执行，告警信息推送等。可以自定义报警策略，对集群节点的系统资源利用情况、网络通讯情况、进程运行情况和集群运行状态等信息进行采集监控，将报警信息推送给用户，使用户及时发现和排除集群故障。

一、采购内容

| 序号 | 名称 | 单位 | 数量 | 备注 |
| --- | --- | --- | --- | --- |
| 1 | 支撑平台运维管理系统 | 套 | 1 | 完成远程教育支撑平台、继续教育学习平台软硬件的运维管理系统开发，功能主要包括：设备管理、服务器管理、应用管理、服务管理、端口管理、日志管理、预警管理、工单管理、系统管理、运维大屏、系统对接等。具体指标见功能要求。 |
| 2 | 数据处理工作站 | 台 | 1 | 类型：台式机<br>CPU：酷睿 i7-12700KF 12 核 20 线程<br>存储：内存 32G D43200、硬盘 NVme 1T 固态 M.2 + 希捷酷鱼 2TB<br>显卡：NVIDIA RTX 3060 12G<br>电源：650W 宽幅稳压<br>散热：静音水冷<br>显示器：双显 27 英寸 4K 超清 65W Type-C 反向充电 |
| 3 | 显示器 | 台 | 8 | 23.8 英寸、IPS 屏、FHD、75Hz、100%sRGB、300nit、低蓝光、智能调光、DP 接口、HDMI 接口、旋转升降 |
| 4 | Wifi6 路由器 | 台 | 1 | 千兆 Wi-Fi6、5400M 无线速率、5G 双频、4x4 MIMO、支持防火墙、支持 Mesh、千兆网口、独立 FEM 数量：6 个、CPU IPQ5018 双核 1G、内存容量：512MB、Wi-Fi 6 |
| 5 | 办公椅 | 把 | 8 | 网布面料、转椅类别、120-155 度(含)靠背、腰背分离、可旋转可升降扶手、座深座高可调、带滚轮，调节式头枕，推拉搁脚、气压升降 |

## 二、服务要求

| 类别 | 指标 | 具体要求 |
| --- | --- | --- |
| 设备管理 | 设备类别管理 | 设备类别如服务器、路由器、交换机、防火墙、VMs 和存储设备，获得它们的状态和可用性的实时信息，实现对硬件 CPU、主板、硬件、风扇、温度等物理状态的监控。<br>支持添加/修改/删除设备类别。<br>支持管理设备类别对应的设备参数。 |
| | 主机监控 | 1、主机管理<br>添加/修改/删除设备，如 PC 服务器及相关设备等。<br>主机添加：由系统管理员主动添加，管理服务器描述信息（名称、型号、厂家等），固定资产信息（选填，如固定资产类型、固定资产编号、价值、购置日期、存放位置等），设置关联的主机管理员，添加后生成配置文件，并将配置文件和 exe 打包成压缩文件。由主机管理员登录系统后点击下载并安装，安装成功后获取并回传主机描述信息如 ip、设备名称、设备类型、操作系统、中间件、服务器配置信息如 cpu、内存等信息。新增主机将会显示在主机列表中。<br>主机修改：由于主机属性均由系统获取，主要修改主机使用状态，可修改关联的主机管理员。<br>主机删除：仅系统管理员可删除主机，主机一旦删除，不再监控，同时更新系统监控拓扑。<br>2、主机监控<br>实时监控，包括 CPU、内存、硬件、网卡、系统关键日志、是否 ping 通。显示主机监控信息列表，查看已授权的所有主机上报的信息，显示主机的系统类型、ip、操作系统类型、内存使用率、cpu 使用率、磁盘剩余量/总量、接收量、发送量、启用时间等，支持查看每台服务器的状态、详细信息、报警信息和监控信息，监控信息包括 cpu 使用率，cpu 温度，磁盘使用率，内存使用率，主机流量，磁盘 IO 等。<br>3、告警通知<br>监控中的主机如有系统负载、磁盘容量、网络、CPU、内存等指标超过告警阈值时，系统自动向主机管理员发送告警通 知，没有主机管理员的直接通知系统管理员。附件显示系统详细信息，如 cpu 使用率、cpu 温度、磁盘 |

| | | |
|---|---|---|
| | | 使用率、磁盘 io 信息、接口情况、端口情况等信息。支持查看对应主机的主机监控情况，查看 CPU 监控图表，查看 CPU 使用率%图形报表；内存监控图表，查看内存使用率网络流量监控图表网络接收发送包监控图表；系统负载监控图表；支持查看系统信息详情，如 cpu 个数、型号、系统类型、磁盘空间、CPU 温度、磁盘 IO 信息等。运维人员处理故障后应记录处理时间、问题状态。 |
| | 虚拟机监控 | 1、虚拟机管理：<br>添加/修改/删除设备，完善虚拟机基本信息（如名称、厂商、型号、cpu、内存、存储等），固定资产信息（选填，如固定资产类型、固定资产编号、价值、购置日期、存放位置等），关联管理员，可选多个虚拟机设置管理员或管理员组。<br>2、虚拟机监控<br>支持通过 API 接口实现对主流虚拟化设备进行监控和管理，包括：VMware 、Hyper-V 等设备管理。监控参数主要有进程内存分配情况、线程参、类加载、主机内存参数等信息。<br>3、告警通知<br>监控中的虚拟机如有系统负载、磁盘容量、网络、CPU、内存等指标超过告警阈值时，系统自动向管理员发送告警通知，没有管理员的直接通知系统管理员。运维人员处理故障后应记录处理时间、问题状态。 |
| | 存储设备管理 | 1、存储设备管理<br>添加/修改/删除设备，如集中式存储、分布式存储管理和备份一体机等。添加设备时主要完善设备基本信息、固定资产信息（选填，如固定资产类型、固定资产编号、价值、购置日期、存放位置等），设置对应的设备管理员，可选择多个设备同时设置管理员或管理员组。<br>2、存储设备监控<br>实现对存储设备的存储 IO 等性能的监控。对存储设备状态监测和管理包括以下重要的内容：存储 IOPS 信息；磁盘空间，可用率，运行状态；电源，风扇状态；控制器状态；对性能数据的采集支持自动化调度的方式，支持 Cluster、Array、Volume 等不同级别的性能监控，能展示设备历史和实时的磁盘性能状况以及 Write I/O Rate、Read I/O Rate、Read Cache Hits、Write Cache Hits、Read Data Rate 等性能指标。 |

| | | |
|---|---|---|
| | | 3、告警通知<br>根据情况给出硬件相关告警信息。设备告警信息主动上报和集中展现，助力运维人员分析判断故障类型以及故障节点，运维人员处理故障后记录处理时间、问题状态。 |
| 服务管理 | 文件管理 | 1、文件管理<br>支持添加/删除/修改文件明细，主要包括服务器 IP、文件名称、存放位置等信息，可设置文件是否需要监控，并关联对应的管理员，支持选择多个文件设置管理员或管理员组。<br>2、文件监控<br>管理文件监控列表，主要监控文件是否被篡改。<br>3、告警通知<br>对于系统发现的被篡改的文件应及时向对应的管理员发送告警通知。运维人员处理故障后应记录处理时间、问题状态。<br>4、巡检记录<br>系统管理员和对应的管理员可点击巡检，完成巡检登记，系统自动记录巡检时文件状态，支持查看对应的巡检记录，巡检记录包含巡检时间、巡检人、文件状态、如有告警信息支持查看详情及故障处理操作。 |
| | 中间件管理 | 1、中间件管理：提供对主流中间件的管理， 包括 WebSphere Application Server、Webspere Portal Server、JBossAS、 Oracle AS、WebLogic、Sun JES、Tomcat、ApusicAS 等 J2EE 中间件；添加时完善基本信息（如名称、版本、厂商等），关联管理员，支持选择多个中间件设置管理员或管理员组。<br>2、中间件监控<br>支持对 Websphere、Tomcat 等中间件进行监控，中间件监控指标主要包括配置信息管理器、故障监控、性能监控。包括名称、版本、监听端口、是否激活、当前连接数、请求数、会话数，被拒绝的活动数、最大数量、性能等指标的监控。<br>3、预警告知<br>中间件发生故障，或性能指标超过设置的预警阈值时，系统自动向管理员发送告警通知，没有管理员的直接通知系统管理员。运维人员处理故障后应记录处理时间、问题状态。 |

| | | |
|---|---|---|
| | 容器管理 | 1、容器管理<br>添加/修改/删除容器，完善容器基本信息（如名称、类别、使用的镜像、创建时间、版本、状态等），关联管理员，支持选择多个中间件设置管理员或管理员组。<br>2、容器监控<br>实现对容器的网络流量、容器数量、CPU、内存、io、cpu 占比、内存占比、运行时间等指标的监控。<br>3、预警告知<br>发生故障，或性能指标超过设置的预警阈值时，系统自动向管理员发送告警通知，没有管理员的直接通知系统管理员。运维人员处理故障后应记录处理时间、问题状态。 |
| | 数据库管理 | 1、数据库管理：实现对 MySQL、Redis、Nigix、MongoDB、Oracle、sqlserver 等数据库的实时监控管理，包括数据库名、版本、并行状态、基本配置等信息。能对数据库进程信息监测：进程占用 CPU 时间、内存大小、数据库进程总数等。能监测数据库会话信息：缓冲区命中率、已连接的用户数、空闲的连接数。关联对应的管理员，支持选择多个数据库设置管理员或管理员组。<br>2、数据库监控：<br>对数据库基本信息、表空间、I/O、CPU 使用率、内存占用率等基础信息持续采样，并以直观的图形化方式展示，快速掌握数据库运行的基本健康指标。数据库列表、指定数据库的表信息、列、索引、数据库和表分别对应的数据分布状况，且这些信息都可以通过条件进行查询。实现对数据库状态、使用量、数据库实例、数据库对象、BUFFER 状况、SQL 会话、活跃事务、阻塞活动、死锁信息、数据库文件等指标的管理。可对其进行相应信息进行操作，添加页面，选择数据源，表别名，sql 语句。<br>（1）数据源添加<br>添加数据源时，需要对其进行相应信息进行输入，包括对数据库类型，用户名，密码，端口，名称、等信息。<br>（2）数据表添加<br>添加完数据源，就可以添加数据表进行监控数据表的数据量了，设置数据扫描时间间隔，按照数据扫描时间间隔统计表数据量。 |

| | | |
|---|---|---|
| | | （3）数据表管理<br>数据表可以随时启用停用监控。<br>单击页面的数据表管理按可打开对应页面可对其进行相应信息进行操作。管理数据库列表、指定数据库的表信息、列、索引、数据库和表分别对应的数据分布状况，且这些信息都可以通过条件进行查询。<br>3、预警告知<br>对数据库以及所在操作系统长期运行状态的分析，确保持续长期运行在优良的运行环境，确保业务的正常运行。对于异常情况应及时向对应的管理员发送告警通知。运维人员处理故障后应记录处理时间、问题状态。 |
| 应用管理 | 应用管理 | 1、进程管理，对应用的使用资源如内存和 cpu，进行实时监控。<br>列表展示 ：点击左侧进程管理菜单，可以查看所有进程的资源占用信息。<br>在进程列表，点击【添加】，跳转到添加进程页面，选择监控主机，输入进程 id，进程名称等信息，然后点击保存。<br>进程添加支持进程 id，pid 文件，进程名称关键字来识别进程。<br>进程可以随时启用停用，启用时候进行监控，停用则不再监控。<br>2、端口管理<br>列表展示：在左侧菜单，点击端口管理，端口也是实时监控，但是端口没有趋势图，只有状态(正常或失败)。<br>端口添加：在端口列表，点击添加，跳转到添加端口页面，选择监控主机，输入端口， 别名等信息，然后点击保存。<br>端口可以随时启用停用，启用时候进行监控，停用则不再监控。<br>3、关联管理员<br>关联对应的管理员，支持选择多个应用设置管理员或管理员组。 |
| | 应用监控告警 | 1、支持对标准 URL 的连通性进行监控，用户可以根据设定的包含或不包含关键字、响应时间来制定相应告警策略；支持将 URL 监测绑定到对应服务器。<br>2、支持对服务端口进行监控，可自定义服务端口。对主机上的 tcp 端口进行 telnet 测试，端口是否开通，如果开通则正常，否则失败，通过在监控主机执行 telnet localhost 端口来测试，因此不用考虑防火墙和网络因素。<br>3、系统支持对不可 SNMP 管理的设备进行 PING 通断性监测；系统支持单条 |

| | | |
|---|---|---|
| | | 和批量添加 PING 目标，PING 目标可以是 IP 或者 URL；系统可以对 PING 参数进行设置，如 PING 次数、PING 数据包长度、PING 超时时间设置；系统支持 PING 细节数据保存时间、统计数据保存时间设置；系统支持循环执行和定时执行两种方式，可设置循环执行的间隔最短至 5 分钟；PING 通断监测异常、恢复时可进行告警。<br>4、运维人员处理故障后应记录处理时间、问题状态。 |
| 日志管理 | 日志接入 | 日志监控主要管理 Mysql 慢日志、Redis 慢日志、系统操作日志、数据库操作日志等。<br>在日志管理列表点击添加，跳转到添加页面，选择监控主机，输入日志文件的绝对路径，或日志文件的目录，告警关键字等信息，设置扫描间隔时间，保存。 |
| | 日志整合 | 当日志文件为目录时候，系统会每次扫描时间戳最新的日志文件，按照设置的扫描间隔时间进行扫描。日志监控可以随时启用停用，启用时候进行监控，停用则不再监控。 |
| | 日志告警 | 设置告警时间间隔后，在告警时间间隔内同一个日志文件不会重复告警，只是不发送告警消息，日志扫描工作仍然在正常进行，可以根据实际场景调整此参数值。每次扫描会记录上一次扫描文件结束的位置，从结束位置继续扫描。<br>如果日志文件被修改或清空，会重新从第一行扫描。 |
| 预警管理 | 预警规则设置 | 1、管理性能基准指标；<br>2、定义报警阈值；<br>3、设置故障处理流程。 |
| | 预警列表 | 1、对资源监控的所有告警信息统计分析，按照告警级别、告警类别、告警类型进行统计。<br>2、按照告警级别统计近 30 日的告警数量趋势。<br>3、支持对各类资源的告警信息按照时间进行查询。<br>4、支持告警清除功能。<br>5、支持设定不监测时间段。<br>6、网络设备监控要求具备报警确认机制，即首次发现故障并不转发报警，根据不同的报警类型再进行不同次数的故障确认，确认为故障后进行报警。<br>7、要求支持 SNMP 无响应、服务端口无响应、进程不存在、关键接口异常、 |

| | | |
|---|---|---|
| | | URL 监测异常、PING 无响应、JDBC 无法连接到数据库、JMX 无法连接到目标服务器、HTTP 无法连接到目标服务器、EMAIL 监测异常等故障类报警；CPU 利用率超过阈值、接口流量超过阈值、温度超过阈值、湿度超过阈值、内存利用率超过阈值、硬盘利用率超过阈值、数据库连接时间超过阈值、数据库表空间利用率超过阈值、数据库缓存命中率超过阈值、Apache 响应时间超过阈值、JVM 利用率超过阈值、IIS 当前连接数超过阈值、已用连接数百分比异常、接口单播包超过阈值、接口广播包超过阈值、IIS 当前用户数超过阈值等阈值类报警；新计算机、IP 地址改变、上连设备改变、计算机名改变等终端类报警。<br>8、支持导出历史告警列表。<br>9、支持查看告警源详情。如告警说明、参考信息、影响范围及处理步骤等<br>10、支持根据监控项类型、产品、服务、等级、状态、开始日期、结束日期及过滤内容来进行过滤查询。<br>11、支持告警处理（如处理中、处理完成、事件跟踪、上报 ITIL 等） 导出告警列表里的告警信息。<br>12、支持告警屏蔽，在告警屏蔽的添加页面，配置需要屏蔽的告警筛选项。支持为已屏蔽的告警解除屏蔽。<br>13、支持搜索关键字查询，如集群、产品、服务、等级、状态、监控项名称等，单击查询，可查询到相应的告警事件。单击各色块可跳转至对应的告警事件页面，可以根据业务需要，查询、添加、修改以及删除告警联系人和联系人组。 |
| | 预警消息下发 | 1、预警消息下发方式：邮件、钉钉、短信、电话等即时通讯方式。<br>2、预警消息下发：根据硬件监控、系统监控、应用监控、网络监控、安全监控、业务监控、日志监控等已关联运维人员的预警消息将自动下发，未设置运维人员的由系统管理员接收预警消息，系统管理员可手动设置预警消息接收对象。<br>3、依据告警策略对运维用户的违规操作进行告警，告警信息至少包括：a）操作时间；b）运维用户；c）源地址；d）运维对象；e）管理方式；f）时间描述；g）触发的策略等。 |
| 运维监控 | 监控大屏 | 支持全网运行状态总览，包含设备运行状态统计、设备厂商统计、最新告警时间、故障设备列表、关键设备 CPU 历史曲线等信息。支持大屏轮播， |

| | | |
|---|---|---|
| | | 自动切屏展示内容。显示主机的监控面板信息以及对应的图表，显示信息包括：监控主机数量、监控进程状态、服务接口数量、监控端口数量。其中主机画像可以对主机的所有指标进行整理统计显示，包括当前和历史的内存、cpu、系统负载、网络流量等信息、监控端口、监控日志、监控进程等信息。 |
| | 性能查询 | 1、对各类资源的性能数据进行记录，并统一查询性能数据，支持自定义查询类型、查询时间，支持对查询指标进行过滤。<br>2、支持对各类资源的性能数据进行 TOP-N 排行查询，至少包含响应时间、可用性、CPU 利用率、流量的性能查询。<br>3、故障 TOP-N 排行、可用性排行可按资源类型进行筛选。<br>4、要求系统提供网络设备表、服务器表、入网计算机表的导出功能。 |
| 系统管理 | 角色管理 | 对系统中的角色进行管理。 |
| | 权限管理 | 对于系统中的角色权限进行设置； |
| | 用户管理 | 添加用户后设定角色，管理运维人员操作权限及关联设备。<br>管理员仅能对用户管理进行操作，包括用户的添加、删除、修改、禁用、启用用户的权限。 |
| | 登录管理 | 系统提供登录入口，实现系统内的登录和退出。<br>实现与在线教育支撑综合服务平台集成项目的对接，可通过统一身份认证入口登录。<br>运维人员登录后查看关联的设备管理列表、服务管理列表、应用管理列表，同时查看预警信息和工单列表。 |

# 附件二：项目其他要求

| 类别 | 子项 | 具体要求 |
| --- | --- | --- |
| 技术要求 | 整体要求 | 系统应支持开放接口，方便新的功能模块的加入；系统需满足招标方提出的以下的所有需求。 |
| | 开发技术 | 系统基于 B/S 架构，服务端开发语言采用 Java、数据库采用 MySql5.6+，支持读写分离、缓存 Redis4+，支持集群，前端采用 html5+css3；操作系统支持 Linux、win8、server2002 以上版本发布环境为 IIS7+ 或 tomcat8+； |
| | 系统部署 | 系统支持 Windows 任何平台及主流 Linux 平台的安装。<br>支持纯 IPV4、IPV6 网络环境，以及 IPV4/IPV6 双栈网络环境。 |
| | 浏览器兼容 | 系统兼容 ie9+、chrome45+、firefox、safari 等主流浏览器。 |
| | 性能需求 | 一台 4 核 8 线程主流处理器、64G 内存的服务器能够满足 2000 并发时关键业务响应不超过 2 秒。系统具有可扩展性，可以通过服务器的扩充，提供更多并发服务。 |
| | 软件结构 | 整体项目结构分为业务消费端,业务提供端,服务管理中心和数据处理中心，彼此之间完全解耦，业务提供端发布微服务到服务管理中心，业务消费端以接口形式从服务管理中心获取具体业务服务地址后调用具体业务微服务，业务提供端处理完业务后以 RPC 协议通知数据处理中心进行数据的增删改查。<br>业务提供端：以微服务为核心，整体拆分为接口和接口实现,以接口为标准将接口实现通过 RPC 协议发布到服务管理中心。<br>业务消费端：通过业务服务端提供的接口以 RPC 协议从服务管理中心获取具体的业务提供端进行业务调用。<br>服务管理中心：记录服务提供端的具体地址和服务标准。<br>数据处理中心：满足主流数据库如 MySql,Oracle 及 SqlServer 的增删改查操作，提供读写分离已经跨库操作并保证日常处理事务,对外提供 RPC 协议进行访问调用。 |
| 对接要求 | 对接要求 | 1、系统对接：需与郑州大学继续教育学院、远程教育学院在线教育支撑综合平台集成项目完成功能、数据和服务无缝对接；接口对接：提供第三 |

| | | |
|---|---|---|
| | | 方接口对接技术支持服务。<br>2、与郑州大学继续教育学院、远程教育学院在线学习平台、移动学习平台、教学管理平台、在线考试系统、在线监考系统、学位外语考试系统、招生报名系统、毕业论文与答辩管理系统、学籍与毕业管理系统、自学考试报名系统、自学考试学位申报系统、母亲学院平台、运维管理系统，实现子系统间的权限对接、登录对接、数据对接、服务对接等。<br>3、与统一身份管理与登陆系统对接；对用户实现统一身份认证，用户一站式的访问登录，通过一次验证之后，可以快捷访问其他的应用系统，无需再次认证。而子系统的用户登录应跳转到统一登录入口。 |
| 服务需求 | 技术支持 | 对各个角色用户提供技术支持； |
| | 服务监控 | 对系统服务、数据库服务器资源等监控和维护； |
| | 驻场要求 | 根据疫情管控实际情况，在学校允许情况下，合同签订后提供一年的驻场开发服务。 |
| | 培训要求 | 中标方应负责对招标方人员进行专业培训，使用培训人数与培训时间由招标方确定。 |
| | 数据库备份 | 对数据库服务器上的数据库进行定时备份及对以前数据的清除； |
| | 服务器资源扩容 | 需要配合学院老师对各服务器进行硬盘空间、内存、CPU 等资源扩容，保证系统扩容前后正常运行； |
| | 完善操作手册 | 完善用户操作手册。 |
| 知识产权 | 知识产权归属 | 项目实施过程中产生的相关文档、软件系统等知识产权成果归郑州大学所有。 |
| 交付要求 | 交付时间 | 合同签订后 30 个工作日内完成软件开发测试和整个系统的部署。 |
| | 交付内容 | 1. 系统设计文档。<br>2. 系统数据库设计文档。<br>3. 系统集成部署设计文档。<br>4. 测试报告。<br>5. 系统用户说明书。<br>6. 系统运维服务计划。<br>7. 用户培训文档。 |

# 郑州大学信息系统建设网络安全责任协议

甲方：郑州大学

乙方：河南丰联信息科技有限公司

甲、乙双方现就郑州大学继续教育学院远程教育学院支撑平台运维管理系统（以下简称“项目”）进行建设合作。根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等相关法律法规和《信息安全技术 网络安全等级保护基本要求（GB/T 22239-2019）》、《信息安全技术 个人信息安全规范（GB/T 35273-2020）》等相关国家标准，本着平等、自愿、公平、诚信的原则，经双方协商一致，就该项目实施及后续合作过程中的网络信息安全责任事项达成本协议。

**第一条** 乙方严格遵守《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等相关法律法规和国家相关标准的要求，执行郑州大学网络安全管理相关规定和办法。

**第二条** 乙方承诺在项目调研、开发、管理、实施、运维、售后服务及后续合作过程中，承担相应的网络信息安全责任。

**第三条** 乙方不得在其提供的软件产品中留有或设置漏洞、后门、木马等恶意程序和功能；如果发现其软件产品存在安全风险时，应当及时告知甲方，并立即采取补救措施。

**第四条** 乙方应采取技术措施和其他必要措施，保障所提供软件产品的自身安全和稳定运行，有效应对网络安全攻击，保护数据的完整

性、保密性和可用性。如因软件产品自身安全问题造成的一切责任和后果（包括法律、经济等）由乙方全部承担。

**第五条** 乙方应当为其软件产品运行所依赖的操作系统、数据库系统、中间件、开发框架、第三方组件、容器等持续提供安全维护，并承担相应的安全责任；在合同约定的质保期内外，均不得终止提供安全维护。

**第六条** 如果软件产品涉及密码技术的应用，应确保密码的使用符合国家密码主管部门的相关要求。

**第七条** 软件产品具有收集用户信息功能的，乙方应当提前征得甲方同意；涉及用户个人敏感信息的，还应当遵守《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规和国家标准的相关规定。

**第八条** 乙方应根据信息系统数据的重要性和系统运行需要，制定数据的备份和恢复策略与程序等。

**第九条** 软件产品应对以下活动进行日志记录，包括权限管理日志、账户管理日志、登录认证日志、业务访问日志、数据访问日志等；提供新闻、出版以及电子公告等服务的软件产品，还应记录并留存用户注册信息和发布信息审计功能；所有日志记录留存应至少保存 60 天记录备份。

**第十条** 乙方应制定针对信息系统的网络与信息安全管理制度，对安全策略、账号管理、密码策略、配置管理、日志管理、日常操作、升级与补丁修复等方面做出规定。

**第十一条** 乙方应制定针对信息系统的网络安全事件应急预案，包括预案启动条件、应急处置流程、系统恢复流程等，并定期对应急预案进行评估和修订完善。

**第十二条** 乙方应对其工作人员的技术行为承担责任，包括：（1）不得在甲方服务器上安装各类与项目建设、运行、维护无关的软件；（2）必须按照甲方提供的安全方式进行信息系统及其运行环境的访问，并向甲方报备访问的 IP 地址；（3）在软件产品上线运行后，未经甲方允许，乙方不得对信息系统及其运行环境进行任何操作；（4）做好所属账号管理工作，防止账号泄露、侵入等事件的发生；（5）履行甲方规定的安全责任相关要求；（6）因乙方工作人员造成的损失由乙方承担相关责任。

**第十三条** 乙方应对软件产品的安全检测、应急响应和安全事件处置承担责任，包括：（1）对软件产品及其运行环境进行定期性的安全检测，并将结果以书面形式报告给甲方；（2）软件产品及其运行环境被检测出或发生安全问题时，乙方须在 1 小时内做出应急响应，并在 24 小时内完成应急处置，防止损失的进一步扩大。

**第十四条** 乙方如若无法在规定时间内做出响应和完成相关安全工作，甲方可自行组织开展相关工作，乙方承担由此产生的所有费用。

**第十五条** 乙方的网络安全责任自本协议盖章之日起开始生效。

**第十六条** 本协议一式三份，甲方建设部门和乙方各一份，报备学校信息化办公室一份。

甲方（盖章）：郑州大学

部门负责人（签字）：

签字日期：2023.1.4

乙方（盖章）：河南丰联信息科技有限公司

法人或授权代表（签字）：

签字日期：2023.1.3

# 郑州大学信息系统建设信息安全保密协议

甲方：郑州大学

乙方：河南丰联信息科技有限公司

甲、乙双方现就郑州大学继续教育学院远程教育学院支撑平台运维管理系统（以下简称“项目”）进行建设合作。根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等相关法律法规和《信息安全技术 网络安全等级保护基本要求（GB/T 22239-2019）》、《信息安全技术 个人信息安全规范（GB/T 35273-2020）》等相关国家标准，本着平等、自愿、公平、诚信的原则，经双方协商一致，就该项目实施及后续合作过程中的数据安全保密责任事项达成本协议。

**第一条** 乙方严格遵守《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等相关法律法规和国家相关标准的要求，执行郑州大学网络安全管理相关规定和办法。

**第二条** 本协议中的“保密信息”是指乙方在项目调研、开发、管理、实施、运维、售后服务及后续合作过程中，对所接触到来源于甲方以任何方式获取、不为公众所知的所有信息、数据、资料和技术等，包括与项目规划有关的建设规划、实施方案、项目合同、其他内部文件等，与运行环境有关的网络拓扑、设备信息、网络协议、部署结构等，与系统开发有关的技术参数、软件架构、开发文档、配置

文档、业务软件及源代码、管理手册、知识产权信息及产品专利等，与运维管理有关的各类设备及系统账号口令、密码管理策略、日志数据、用户手册、内部管理规章制度等，与业务数据有关的教职员工、学生、注册用户等个人信息以及教学、科研、管理、办公、财务、人事等业务数据。乙方以任何形式全部或部分从保密信息中获得的任何信息、数据、资料和技术等均被视为保密信息。

虽然不属于上述所列情形，但信息、数据、资料和技术自身性质表明其明显是保密的。

**第三条** 乙方保证该保密信息仅用于与双方合作项目有关的用途或目的。未经甲方同意，乙方不得对保密信息进行复制、修改、重组、逆向工程等，不得利用保密信息进行新的研究或开发利用。

**第四条** 未经甲方同意，乙方不得向任何第三方传播或披露甲方的保密信息。

**第五条** 乙方应采取必要措施保护和妥善保存从甲方获知的保密信息，防止保密信息被盗窃和/或泄露，乙方保存保密信息的存储介质应由乙方指定的专人进行管理，并向甲方报备。

**第六条** 乙方不得刺探与本项目无关的甲方保密信息。

**第七条** 保密信息仅可在乙方范围内仅为项目之目的而使用，乙方应保证相关使用人员在知悉该保密协议前，明确保密信息的保密性及其应承担的义务，并以书面形式同意接受本协议条款的约束。乙方应对上述人员的保密行为进行有效的监督管理，如发现保密信息泄露，应采取有效措施防止泄密进一步扩大，并及时告知甲方。若乙

方上述人员出现岗位调动或离职的情形，乙方有义务立即通知并配合甲方终止其与甲方有关的信息访问权限，收回其所持有的甲方保密资料和涉密介质，并确保该人员在离职后继续履行好保密义务。

**第八条** 存有保密信息的存储介质如需送到单位外维修时，要将涉密资料备份后，对介质进行技术处理，以防泄密。

**第九条** 乙方所承担项目建设工作完成后或中途不再从事本项目相关工作，不得保留任何保密信息的副本。

**第十条** 甲乙双方一致认同，对于本协议签订及履行过程中、项目的商谈及合作过程中所接触到的甲方及其所属单位所有机构的保密信息，乙方应根据本协议约定履行保密义务、承担责任。

**第十一条** 乙方同意：若违反本协议书内容，甲方有权制止乙方行为并要求其消除影响，视行为严重程度进行处罚；后果严重者，甲方将通过法律途径要求乙方进行经济赔偿，并向司法机关报案处理。

**第十二条** 乙方的保密义务自本协议盖章之日起开始生效。

**第十三条** 乙方的保密义务并不因双方合作关系的解除而免除。

**第十四条** 本协议书一式三份，甲方建设部门和乙方各一份，报备学校信息化办公室一份。

甲方（盖章）：郑州大学

部门负责人（签字）：

签字日期：2023.1.4

乙方（盖章）：河南半联信息科技有限公司

法人或授权代表（签字）：

签字日期：2023.1.3