

**郑州大学信息化办公室、网络管理中心郑州大学网站群平台
安全升级采购项目
采购合同**

甲方（全称）：郑州大学

乙方（全称）：西安博达软件股份有限公司

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》及有关规定，遵循平等、自愿、公平和诚实信用的原则，双方就郑州大学信息化办公室、网络管理中心郑州大学网站群平台安全升级采购项目及有关事项协商一致，同意按照下述条款订立本合同，共同信守。

一、 供货内容及分项价格表

1、 本合同所指供货内容详见附件 1，此附件是合同中不可分割的部分。

2、 本合同总价款为人民币（大写）叁拾肆万陆仟捌百元整（¥346800元），供货内容的分项价格表详见附件 2，此附件是合同中不可分割的部分。合同总价中包括软件购置费（含授权费）、开发服务费、安装部署费、调试费、各类检测费、运行维护费及培训所需费用及税金，甲方不再另行支付任何费用。

二、 服务约定

1、 交货时间：10 日历天。

2、 交货地点：校方指定地点。

3、 交货方式：现场交付。

三、 质量要求或服务标准，乙方对质量负责的条件和期限

1、 基本要求

(1) 甲乙双方在签订合同的同时，须与项目建设部门签订《郑州大学信息系统建设网络安全责任协议》（附件 3）和《郑州大学信息系统建设信息安全保密协议》（附件 4）。

(2) 乙方须按合同要求提供符合招标标书要求的产品，且应达到乙方投标文件及澄清文件中明确的技术标准。甲方如果发现乙方所供产品不符合合同约定，甲方有权单方解除合同，

由此产生的一切后果由乙方承担。

(3) 乙方负责在项目完成后将项目实施所涉及的全部相关技术文件资料（包括但不限于信息标准集、需求说明书、数据表结构、系统详细部署文档、本项目实施中产生的所有开发源代码、全部接口技术文档、后期应用系统相关接口等），以及系统测试、验收报告和系统测试使用的测试数据等文档汇集成册提交给甲方，并提供所有资料的电子文档；同时，提供本项目所有软件产品和数据资源的电子文件。

(4) 乙方负责在项目完成后对甲方人员进行免费的系统运维、二次开发等涉及项目后续发展的有关技术培训。

(5) 乙方应提供完整的项目实施计划、详细的工作内容安排及过程控制和验收方案等。

(6) 乙方应保证甲方在使用其所提供的产品时免受第三方提出侵犯其专利权、商标权或保护期的起诉。

(7) 本项目中甲方定制开发部分，其软件著作权归甲方所有。

(8) 其他：无。

2、项目人员配置

(1) 乙方应针对本项目成立由项目经理带队的不低于10人的项目团队，其中实施期驻场人员不应少于1人，并建立保障本项目顺利实施的各项管理制度和质量保证体系。为了保证项目实施的连续性，项目实施过程中应至少保证2名以上核心技术人员不能更换。

(2) 乙方应在项目实施方案中提供项目组成员名单，并详细描述项目组成员的技术能力、项目履历、工作职责和具体工作内容等。

(3) 其他：无。

3、进度要求

乙方应针对本项目提交项目实施计划，经甲方确认后严格按照计划执行，并按计划要求交付产品和成果。如需变更必须提出书面的实施计划变更手续。

4、开发管理

乙方应对项目实施进行科学严格的管理，能够对项目进行系统计划、有序组织、科学指导和有效控制，促进项目全面顺利实施。

5、文档管理

乙方应根据开发进度及时提供有关开发文档，包括但不限于需求说明书、系统设计说明书、测试计划、测试分析报告、系统部署手册、操作手册、系统安装手册等。

6、用户培训

乙方对甲方人员的培训应贯穿于整个项目的实施过程中，包括从项目准备、研发到项目运行维护和使用的全过程。乙方提供详细的培训方案、培训内容、培训计划、人员数目、开发工具、软件使用和后期维护等。

(1) 培训内容

1) 乙方应对甲方人员进行系统的研发管理培训，即项目开发的各阶段技术培训，具体包括但不限于项目准备、用户需求分析、系统概要设计、系统详细设计、程序编制和运行建立等。

2) 乙方应对甲方人员进行系统的技术培训，使甲方人员能掌握项目相关系统的使用、维护和管理方法，能独立进行系统使用、管理、故障处理、日常测试和维护等工作，以保证所建设的系统能够正常、安全、平稳地运行。

(2) 培训要求

1) 培训教师应具有丰富的应用实践经验和教学经验，中文授课。

2) 乙方提供培训使用的文字资料和讲义等相关材料。

3) 如果培训地点在外地，乙方应向甲方承诺为所有培训人员提供食宿。

(3) 培训方式

乙方根据培训内容提供不限于课堂讲解、实际操作、专题交流、现场实施指导等培训方式。

7、产品运行支持与服务保证

质量保证期内乙方提供免费上门服务，服务内容包括但不限于软件系统和数据资源的维护、优化、升级、服务响应、使用培训等。质量保证期内，自接到甲方的故障报修后，乙方2小时内派遣专业技术人员到达故障现场，技术人员在24小时内解决问题，直至软件系统正常运行及相关资源正常使用。

四、验收标准、方法

(1) 由乙方提供相应软件产品的安全合格报告或证书。

(2) 由乙方提供相应软件产品的安装配置文档、运行维护文档和用户使用指南等相关验收资料。

五、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：

项目产品验收合格并经审计后，甲方向乙方支付合同总价款的85%，即人民币贰拾玖万

肆仟柒佰捌拾元整（¥ 294780 ）；剩余总价款的 15%作为后续优化服务履约保证金一次性扣留，即人民币伍万贰仟零贰拾元整（¥ 52020 ），优化服务期为 3 年；第一年结束后，甲方对乙方所提供服务的质​​量进行阶段评价，合格后支付合同总价款的 10%，即人民币叁万肆仟陆佰捌拾元整（¥34680 ）；第三年结束后，乙方服务质量合格，甲方向乙方支付剩余合同总价款的 5%，即人民币壹万柒仟叁佰肆拾元整（¥17340 ）。

六、免费质保约定

1、 免费质量保证期为自项目验收合格之日起三年，质量保证期内乙方提供免费上门服务 and 7×24 小时全年无休电话服务，服务内容包括但不限于软件系统和数据资源的维护、优化、升级、服务响应、使用培训等。

2、 质量保证期内乙方对产品提供 7×24 小时全年无休的安全运维监测和告警服务，并提供专业的解决方案建议。乙方每月进行一次安全检测和病毒扫描，及时调整安全策略和安全规划，备份重要数据，升级系统和安装补丁等。

3、 其他：无。

七、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：400-605-1065

4、质保期外服务：

乙方承诺提供质保期外的 有偿 服务，所提供服务与质保期内服务相同，并承担同样的责任与义务。质保期外服务须另行签订合同。

八、履约担保

合同总价款 10 万元及以上的，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。

九、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 5% 向甲方支付违约金。因为乙方原因造成合同迟延履行，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，按有关规定承担违约责任。

十、其他

1、组成本合同的文件及解释顺序为：投标书（响应文件）及其附件、本合同及补充条款；招标文件（采购文件）及补充通知；中标（成交）通知书；国家、行业或企业（以最高的为准）标准、规范及有关技术文件。

2、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。

3、本合同未尽事宜，由甲乙双方协商后签订补充协议，与本合同具有同等法律效力。

4、本合同共26页，一式12份，甲方9份，乙方2份。招标代理公司1份。

5、本合同由双方签字盖章后生效，合同签署之日起至合同内容执行完毕为本合同有效期。

甲方（盖章）：郑州大学

法定代表人或授权代表：李亚明

单位地址：河南省郑州市科学大道100号

电话：0371-67783088

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：2022年12月26日

签约地点：郑州大学

乙方（盖章）：西安博达软件股份有限公司

法定代表人或授权代表：严亚朋

单位地址：陕西省西安市高新区锦业路125号第201幢13层

电话：029-81021800

开户银行：招商银行股份有限公司西安分行营业部

户名：西安博达软件股份有限公司

账号：291082930810001

签订日期：2022年12月15日

附件 1:

供货内容、技术规格参数及主要功能性能描述

序号	供货内容类别	子系统/功能模块名称	具体技术规格参数、主要功能、性能及配置描述	单位	数量
1	总体技术要求	基本要求	系统采用 B/S 结构设计，基于 J2EE 技术体系和 XML 技术标准开发设计。采用 Java 编程语言和服务端 Java 技术 EJB、Servlet 实现业务逻辑；采用面向对象对象的组件技术，并基于跨平台业界标准；提供面向服务的框架。	/	/
			本系统采用 Java 技术开发，利用 Java 良好的“与操作系统无关”的特性，系统支持与运行环境和开发平台的无关性，充分保证可移植性、安全性、可伸缩性、可重用性。系统具有如下的兼容性：操作系统：支持 Windows（Win10、Win7、WindowXP、Windows Server 等）、Unix、Solaris、Linux（Redhat、CentOS、Ubuntu）、macOS、AIX、优麒麟、中标麒麟、银河麒麟、中科方德、深度等多种主流服务器操作系统。		
			应用服务器：支持 Tomcat、Apache、WebSphere、WebLogic、Jboss 等多种传统中间件，也支持东方通、金蝶、中创等国产化中间件。 数据库：支持 Microsoft SQL Server、Oracle、Sybase、MySQL、IBM DB2、PostgreSQL 等传统数据库，以及达梦、神舟通用、人大金仓、南大通用、瀚高等国产化数据库。 在初始安装部署时，系统内置可以商用的应用软件 Tomcat、Apache 及数据库软件 PostgreSQL，可根据学校要求替换为学校购买的其他商用产品。 系统能够全面兼容主流浏览器，包括可以在微软 IE、微软 Edge、谷歌 Chrome、360 浏览器、搜狗浏览器、苹果 Safari、UC 浏览器、QQ 浏览器、火狐 Firefox、欧朋 Opera 等多种浏览器上访问。无需安装其他特殊插件，系统即可正常使用。 系统既支持 H5+CSS3 自适应技术的网站移动化建设和微网站建设，也提供更加灵活、便捷的多屏展示技术进行网站的移动化建设，实现网站对移动设备的自适应。能够实现网站页面和文章内容、视频、图片等资源的全适配，兼容全部主流智能手机的操作系统：包括苹果 IOS、安卓 Android、		

		微软 WindowsPhone 等，兼容不同设备的分辨率。 系统具有完善的权限和用户管理体系，可以适应学校各类角色管理员的管理和使用，提供与统一身份认证及人事系统的数据接口，并具有集成能力。 平台使用灵活方便，提供 XML、JSON、web service、RSS 等标准接口，为信息采集、聚合提供多种方式。 系统后台数据库及表结构字段清晰易懂，有明确的注释标记，便于进行二次开发和系统扩展。 系统提供网站/新媒体管理和系统管理两种登录入口，分别实现网站/新媒体管理员和系统管理员，支持审计管理员登录入口，实现安全审计管理。系统具有完善的管理操作、入侵防护日志管理功能，便于进行安全审计管理。日志保存 6 个月以上，满足《网络安全法》要求。 系统支持单服务器部署、双服务器部署、多服务器部署、虚拟化部署、管理机与发布机的分布式部署、物理隔离部署和远程分离式部署等多种部署方式，可根据学校实际情况选择不同的部署方式。 系统支持实现动态服务器和静态服务器分开部署， unlimited 静态服务器的数量，动态服务器故障不会影响静态服务器对外提供网站访问服务。 系统具有在线补丁更新机制，可以实现在线安全性加固和升级。无论是对于紧急高危漏洞，或是对于日常性系统升级补丁更新，公司通过在线推送补丁，管理员在收到相关消息提醒后，在线下载安装补丁，从而实现在线的漏洞修补和系统升级服务。同时，系统提供手动更新功能和更新日志记录功能。 系统支持虚拟目录和虚拟主机方式，支持离线/连线状态下的篡改保护，确保网页安全。 系统已默认全面支持针对 IPv6 提供访问支持，Apache 服务可以同时监听 IPV6 和 IPV4 地址。同时支持基于 IPv4 和 IPv6 地址的访问控制，访问记录及统计。符合国家《推进互联网协议第六版（IPv6）规模部署行动计划》要求。 系统全面支持 HTTPS 安全传输协议，具备 SSL 加密通道能力。		
2	网站群综合管理平台	网站群管理	1、站点管理 系统提供对站点进行新增、删除、停止、发布、域名设置等功能，并提供网站检索、网站排序功能。 站点管理功能支持多站点的注册，各站点相互独立，可以配置各站点的目录、模板、工作流程、域名和用户管理等，所有站点使用一套软件统一管理，各站点可以有独立的域名、Logo、栏目结构、套	1

			功能组件、风格模板和后台管理。 系统支持管理权限的逐级授权，如管理员经过系统管理员授权后，自己可以再创建、管理子网站，同时可以进一步向子网站授权。每一个站点可以管理其下属站点、设置站点管理员、设置站点相关属性及其站点之间内容投递关系。 每一个站点可以设置自己的主域名，子站点支持在上级站点下以虚拟目录的形式发布，也可以支持独立域名或二级域名。 平台内各上下级站点有明确的从属关系，各级站点展示和管理方式直观，可以通过平铺图标或树状结构的形式展现，便于管理员管理网站和对其下属子站进行配置和调整。 系统具有主站和子站之间的信息传递机制，能够打破存在于各网站间的信息孤岛，支持不同站点之间的数据共享，除了提供基于相同管理范围内的内容树共享的模式外，还支持站点之间信息推送、跨站发布、跨站引用等信息共享模式，方便网站之间打破信息孤岛。 为了为客户提供更好的应急功能，系统内置了一键关停，可以对站群内的网站快速进行关停，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。 本系统站点管理功能能够实现批量停止维护、停止浏览、停止维护 and 浏览、正常等多种管控模式。 本系统的网页能够全部采用静态化发布，支持组件级的网站和网页动静态发布；并且支持发布多线程，对于静态网站，更新的信息不需要发布整个网站就可以更新到网站上。系统采用的 Cache 缓存机制，可以极大的提高网站的性能，降低对服务器的负载，提高用户访问速度。 同时，系统支持网站动态发布，即对于个性化定制开发功能，也可以选择动态模式即时生成 JSP 动态页面。网站可以根据需要灵活的设置发布方式，支持全部发布、快速发布。支持动静结合的部署方式，动、静态可分开部署，当动态服务器出现故障时，静态发布页面可正常访问；可实现所有站点静态页面同时发布到一台或多台服务器上，或不同站点的静态页面发布到不同的服务器上；静态页面自动生成，在对站点模板、栏目或文章做任何修改后，静态页面能自动增量更新，无需手工触发。 在特殊时期，网站可切换至学校内运行，提升网站安全性能。 2、用户权限与角色
--	--	--	--

		系统支持对所有用户的统一管理，可设置其能够管理的网站及所属部门或组织机构。 系统具有分级、细粒度的权限划分，可以针对不同功能、模块、栏目、文章设置不同的用户管理或访问使用。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，实现权限的细粒度划分。 系统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，实现角色权限划分。 系统支持对部门进行管理，可配置部门相关基础信息，进行增删改等相关操作，可以设置部门相关联站点。 系统可通过设置系统关注人，实现包含：系统备份、系统体检、应用防火墙、运维监控、系统补丁、系统授权监控、防篡改、危险文件扫描等信息的推送和提醒。
		系统采用模板、栏目、资料分离的模式进行网站的创建，其中模板定义网站的表现形式；栏目内的信息可以自由地从平台中提取并组合，而展示采用模板技术，通过修改模板就能完成站点的风格改版和更新。后台资料添加不会影响前台页面的正常展示。 系统支持一键扒站功能，可将某一指定网站原样导入至网站群后台，下载页面文件、图片、样式表等数据，并保持页面样式和兼容性。从而实现网站的原样快速迁移。 系统支持在网站建设过程提供历史数据还原功能，避免修改错误导致页面无法正确恢复。 系统支持采用非破坏性的多屏适配技术，对已有网站或单个页面进行全部或局部移动化，原有网站组件不需要重新配置，可以自动继承，网站建设所见即所得，网站预览提供设备模拟器，支持多种手机分辨率展示效果，确保发布页面的准确性和兼容性。 系统提供通过真实手机扫描二维码进行网站页面效果实时预览功能，从而提供更加真实的效果预览环境。并且二维码的有效期仅供一人使用，保障安全。 系统支持资料自动检测，可快速检测到未配置内容的网站组件，同时进行快速资源配置。
	网站建设	系统为所有用户提供统一的登录界面和用户操作界面，为用户提供“个人桌面”功能，可根据不同用户的使用权限，实现个人工作聚合，“个人桌面”可根据用户个人习惯自定义配置、拖动，支持设置快捷方式，用户可快速跳转至对应模块进行管理。 系统具有简单、稳定、易用的文章编辑器，并且具有 Word/Wps 文档一键原样在线导入，支持 office
	内容管理	

			(word、excel、ppt 等) 文档、PDF 文档内容原样导入，导入后的格式、字体不发生任何变化。 系统支持内容编辑器内对网络文本的采集，能够采集对应的 URL 网络内容资源，直接添加进文章不同字段区间。 系统提供的文章编辑一键排版工具，一键排版功能支持多种预设样式，可在后台下载并参考样例来定义样式文件，自主上传录入排版样式文件，文档可按照预先自定义的格式进行排版。 文章编辑器支持一键排版快速进行文章格式二次排布，一键排版功能支持多种预设样式，以及自定义样式，文档可按照预先自定义的格式进行排版，可以对文章内容源代码进行规范化整理，实现通用性的自动设定文章段落缩进、段间距、行间距、去除空行、多余表格、隐藏域等，确保多种浏览器可兼容。 系统文章编辑器支持在编辑 PC 版内容的同时，可以同时创建手机正文，移动版正文可以从电脑版导入，也可独立编辑，移动版图、文、影可以在电脑版的基础上进行内容清洗，清洗成适合移动设备展示的内容，同一个文章，可以实现不同的展示内容。 系统支持新闻缩略图在系统中多比例裁剪，可设置比例随意拖拽，支持多种旋转翻转模式。 系统支持 flash、pdf 发布。用户可以对红头文件、重要的通知公告等这类文件在后台选择以 flash 或 pdf 的方式进行发布，用户只需要在后台内容编辑界面选择 flash 或 pdf 发布，就可以将编辑好的 Word 文档直接转换成 flash 或 pdf 的格式上传上来。用户无需自己进行转换就可以完成整个过程。 系统能够实现站群级别、站点级别的文章扩展字段自定义。 系统支持新闻时效性管理，管理员设置新闻上下线时间后系统会根据实际自动操作，有效提升管理员的工作效率。 系统支持专题文章检索功能，可以针对某类专题关键字进行相关文章检索，将同类文章快速发布至专题网站或专题栏目下。 系统支持新闻访问权限管理，可以设置单篇文章的访问 IP 规则或可访问角色。 系统支持栏目访问权限管理，可以设置某个网站栏目的访问权限 IP 规则或访问角色权限。 系统提供文章归档功能，当网站文章数据达到一定数量后，可将暂时或永久性不用的文章整理到归档库中，以提升网站前台加载速度、提高网站访问效率、提高文章后台管理效率。管理员可自定义
--	--	--	---

			数据归档条件将站群系统内的数据进行归档。 文章编辑器会自动对文章进行自动保存形成历史版本记录，定时对文章进行保存形成草稿，在草稿箱中可以调用草稿文章，避免浏览器崩溃或其他原因引起的文章内容丢失。 系统除提供常见的按发布时间排序，将文章设为头条、置顶状态外，系统为用户提供可视化的自定义排序功能，即管理员可使用鼠标拖拽的方式进行可视化的、灵活的文章顺序排列。文章顺序被调整后，前后台无需重新发布自动保持一致，可满足不同情况下的不同文章排序要求 系统支持文章发布时投递功能，文章发布时，可将同一文章同时发布到本站点/跨站点的一个/多个栏目中，也可将不同站点不同栏目中的文章同时发布到一个或多个栏目中。 系统支持记录详细的整体站群文章操作日志，可以记录站群系统中被操作文章的网站名称、网站账号、操作者账号、姓名、IP 地址、操作时间、操作内容、操作类型等信息，支持按照站点和操作类型进行查看，并具有查询功能，同时支持以 Excel 文件导出，使得每篇文章内容操作都有据可查，保障站群中所有站点内容安全。 系统采用可视化审核流程生成模式对信息发布的 workflow 进行定义，用户通过拖拽就可完成整个审核流程的设定，处理各种发布信息。流程节点实现拖拽功能，管理员可以设置节点，定义每个节点的审核人员以及下一节点的流转。审核流程的设置支持串联审核和并联审核，每个审核流可以配置相应的栏目，不同栏目可设置不同的审核流，以满足用户信息审核的多种需求。审核的具体操作包括采编、提交审核、审核、退回、发布等，其中审核可设置多级审核，如初审、二审、终审等，审核的层级不受限制。支持查看被审核文章当前的审核状态及处理人、处理意见等相关信息。 网站群数据具备云存储特性，相同文件（资源文件、备份文件等）物理上只存一份。 网站群提供“云文件库”功能，系统针对个体用户提供了“我的文件”用于存放私有文件，针对整站用户提供了“公共文件”用于存放共享的文件。用户可以管理使用个人文件，同时可以查看其它管理员共享的公共文件。 系统支持上传视频时自动进行转换和压缩。系统内置视频转换器，可将文件格式包括：wmv、3gp、mpg、flv、rmvb、mkv、avi、asf、wma、asx、rm、ram、mov 等主流的视频格式转换为互联网最流行的 mp4 格式，在上传过程中提供清晰度及适配设备的选择，满足各类不同的设备访问。上传过程支持单个上传和批量上传，支持断点续传。
--	--	--	---

		系统内置消息体系系统，消息可分为个人消息和系统消息，管理员可根据需求来自定义接收消息类型，并且具有选择多种接收方式，如消息接收或者邮件接收，确保管理员及时获知消息详情。 系统提供信息采集功能，支持 web 采集与数据库采集两种方式。通过对互联网指定网站进行扫描和监控，将指定网站的内容采集到本地系统中；信息采集模块还包含数据库采集系统，通过通用的接口从其他业务数据库中导入信息到本网站中。利用信息采集功能，使系统能对通过第三方数据库，或者对指定网站、版块或栏目进行自动搜索和信息采集。 系统提供完善的跨站点全文检索功能，可实现站群系统内多个网站大量信息资源的检索及管理。提供多种检索方式，包括关键字检索和高级检索。用户可以在任意网站群站点中搜索网站群内部的信 息，全文检索可检索至文章附件正文内容。 管理员在进行文章编写保存和发布时，系统能够自动按照敏感信息词库进行检测分析，并提供敏感信息的快速修正，在事前保证内容安全。 系统支持在文章审核界面对待审文章中存在的敏感信息进行提示，方便审核人对内容进行快速审核，提高审核效率。 系统支持针对敏感信息进行快速处理，支持分别从文章、附件（word、excel、非图片类 PDF 等）、评论、栏目、模板、图片等不同类型的内容进行精准搜索敏感信息；并支持常见敏感信息的快速撤稿或脱敏处理，如工作证、身份证、手机号、邮箱等。同时提供两种检索方式支持站群检索以及数据库检索两大方面，确保内容安全。 系统后台支持设置对敏感词的检测类型，能够有针对性的针对禁用词、慎用词、隐私等进行选择，确定检测范围。 系统针对敏感图片提供基于人脸识别技术的“以图搜图”功能，可以将文章内容中涉及到某人的相关文章筛选出来，进行人物图片文章快速撤稿或脱敏处理。	
	统计分析	系统提供详细的统计分析功能，具有时段访问量统计、各站点信息量、管理员信息量、IP 访问量统计（过滤相同 IP 地址）、文章访问量统计、页面访问量统计、访问来源统计、浏览器统计、操作系统统计、分辨率统计等。支持对统计结果以柱状图、饼状图等多种方式展示。 访问日志统计对所有的访问者信息进行统计，并在网站上进行显示。我们可以方便地看到我们的访问人群都是来自哪个地区，哪个时区是我们的访问高峰期，哪些页面的访问量比较大，针对这些信	

		息我们可以分析我们网站，优化网站，从而提高网站的访问量。 系统支持针对网站内容的相关数据统计，包括网站管理员信息量、栏目信息量、分组信息量、栏目新闻数、网站在线管理员等数据的统计。 站群提供统计功能，可统计系统中的访问记录，包含站点访问量、站点栏目数量、站点/站群文章数、站群在线管理员等。站群提供完整的站群数据统计分析功能，对站点的访问量、发文章、栏目数、投递数、站点接收信息量等，进行统一监管，方便管理员对各部门网站的管理考核。	
		1、数据安全备份与恢复 系统提供独立的远程异地备份系统，用户使用独立的后台就能实现登录及备份快照管理和恢复，支持增量备份，可以针对快照文件快速生成备份包，进行整体系统快速恢复，恢复过程可针对数据单独恢复或对网站数据及模板进行全恢复，保证数据的完整程度。在备份同时提供备份包完整性的检测功能。 网站群系统具有站点恢复功能，子站不需要单独备份，可直接使用系统备份文件实现抽取式恢复。 系统为用户 提供备份包自动清理功能。用户可以通过设置清理策略，系统会根据策略定时自行清理掉不需要的备份包，节省磁盘空间占用，避免资源浪费。	
	安全防护	2.安全防护措施 系统支持密码强度规则设置，并且提供简单密码口令库，对密码进行统一查看、管理维护。使用简单口令库中的密码在创建用户时系统会自动阻止。系统支持用于帐号被盗或忘记密码等的强制修改用户密码，保证帐号安全。采用国密算法，保障密码不被暴力猜解。 系统具有 IP 规则设置和帐号安全管理功能，管理员可以设置不同的 IP 范围，用来限制管理员后台登录，支持对管理员规则进行五级强度设置，支持强制修改弱口令用户密码，保证系统登录安全。 系统内置软件级的应用防火墙，内置被动防御策略集，能够有效阻止 SQL 注入、XSS 跨站脚本攻击、密码猜解，针对危险行为进行 IP 封禁、帐号冻结，并可管理黑名单及白名单，并记录行为和入侵防护日志，降低网站安全风险。通过使用入侵防护日志，可以详细了解攻击者的归属地、IP 地址、攻击位置、攻击特征以及攻击时间等重要信息。 系统提供危险文件扫描功能，只需一键点击扫描即可对站群系统进行扫描，便于及时发现隐患。危险文件的存在给服务器带来严重的安全威胁，经常扫描可以帮助管理员及时发现危险文件，定位危	

		险文件，给系统漏洞修复工作提供信息参考，使服务器能够稳定、安全地运行。 扫描服务器中包含特殊代码的文件，并提供扫描日志，同时允许手动、自动更新危险网站黑名单及信任网站白名单，使服务器能够稳定、安全的运行。 系统支持站群体检功能，对网站群平台运行状况进行危险项目、安全项目等进行全面检测，能够对平台存在的隐患进行排查，并能根据提示做相应处理，提高站群系统安全防护，保障平台安全 系统内置先进的实时网页防篡改系统，可在网站群平台中对防篡改功能的防护能力进行设置，防篡改设置共有三个等级，分别是：强力防护、基本防护、关闭防护。不同防护的等级对站点的安全防护程度不同、对系统资源的占用情况不同以及对站点页面的检测周期时间也不同，支持批量防篡改配置。能够给网站群整体运行、管理和维护提供保护体系。 系统支持 SSL 协议对用户名和密码的传输进行加密，保证关键信息的通信保密性。	
	安全中心	1、安全预警 系统提供统一的安全中心管理，可提供安全预警功能。可展示网站群系统部署结构，完整结构包含终端、发布机（多个）、运行机、管理机、远备、冷备、数据库等，可以展示各服务器运行状态及相关参数，方便管理员直观查看系统运行整体情况 系统提供展示安全防护项功能数量、敏感词库数量、攻击防御数量、近 7 日完整备份包，其中敏感词库可以进行云端更新。 系统具备自动预警及检测机制，以及自动预警系统运维情况，点击运维情况可以进行对应的安全操作。 系统可展示安全相关资讯，系统可以不定期获取云端安全资讯内容，方便管理员及时了解安全相关动态。 2、安全防护控制 系统提供安全防护统一控制功能，包括系统防火墙、web 应用防火墙、用户访问控制等。能够对安全选项统一控制，统一详情查看。 安全防护控制提供文件防火墙、sql 语法检查、网页防篡改、sql 注入防火墙、xss 防火墙、dwr 防火墙、webservices 防火墙、异步请求防火墙、网站访问 IP 封禁、账号冻结、强制修改密码、弱密码、人脸识别登录等安全防护项目的统一控制。通过系统防火墙、主动防御、WEB 应用防火墙、	

			用户访问控制这 4 层安全防护体系。 对于安全防护功能，可以根据已开启、未开启的开启状态进行筛选，便于查找。 3.系统运维监控 系统提供统一的系统运维监控功能，支持查看管理机、发布机服务器（多台）的运行状态，了解资源使用情况。 服务器运行状态情况包括展示服务器 CPU、内存、应用内存、磁盘空间及剩余情况等使用状态，提供进程、操作系统信息等内容的展示。 系统支持查看和导出历史使用状态数据，进行更加细化的分析和长期的留存。 4、日志分析 系统提供全面的日志分析功能，可展示近 7 日志分析情况查看，针对操作日志可以查看异常时间段登录次数，针对 IP 封禁日志可以查看到封禁 IP 数，针对入侵防护日志可以查看攻击最多 IP 地址及防护次数统计，针对敏感词信息可以查看检测出的禁用词、慎用词、错别字、疑似隐私信息等敏感信息数量。同时支持防篡改日志的查看。 系统能够根据日志信息可以展示最新的日志内容。 支持进行所有日志明细的统一查看，包含操作日志、IP 封禁日志、入侵防护日志、敏感词检测日志、防篡改日志等。 我公司提供内容安全管理帮助用户解决网站群平台中内容安全报告问题处置、管理问题，确保已发现的内容安全隐患问题处理的时效性，提升学校网站内容安全问题的处置能力。 我公司提供内容安全管理具备内容安全报告的问题导入、紧急撤稿、任务跟踪与下发、一键验证等安全问题的全闭环可视化。 我公司提供内容安全管理具备内容安全报告问题导入功能，可将扫描服务报告或经编辑处理后的第三方内容安全扫描报告快速导入系统，并对已导入的报告进行任务问题范围确认。 我公司提供内容安全管理具备紧急撤稿功能，能够对网站已发现的内容安全问题做出紧急处理判断，针对需要系统紧急处理的问题提供一键撤稿、一键删除、批量替换等功能。 我公司提供内容安全管理具备任务跟踪与下发功能，系统对网站导入的内容安全问题下发站点处置，二级站点端管理员收到实时的告警提醒，包括系统内通知、邮箱通知等告警提醒方式。站点
		内容安全管理	

			管理员快速、精准地对已发现的内容安全问题进行处理，处理方式包括任务问题范围确认、任务分派与下发（下发二级学院或职能部门）、进度可视化处置看板、任务过程实时跟踪。实现处置任务分派、处置情况查看、监控整个处理过程和进度。 我公司提供内容安全管理具备一键验证功能，支持提供内容安全问题处理验证功能，问题被处理后系统提供二次扫描验证，确保彻底处理，同时支持处理报告数据的导出。		
			1、我公司提供信息发布前提供预先检测服务 我公司所提供的预先检测服务支持对平台发布的信息进行事前在线检测，提高平台输入信息的安全防范能力。并支持对学校网站发布内容检测。 所提供的预先检测方式支持文本检测和网址检测。文本检测支持对将发布的文本内容粘贴复制到系统内一键检测；网址检测支持对网站等地址链接复制到系统内直接检测； 我公司所提供的预检检测能力包含：敏感词、异常链接、疑似隐私信息、易错字及重大表述错误等内容信息。所提供的敏感词库包含但不限于落马贪官、校内敏感词、隐私信息、恐爆违禁、政治敏感、色情低俗、重大表述问题、自定义词库等。本次项目所建设平台系统具备丰富的敏感词库容量，涵盖新华社词库及供应商自有沉淀词库，实现内容发布事前预检。 我公司所提供的检测能力范围如下： 敏感词检测：恐暴违禁、恶意宣传、文本色情、政治敏感、低俗辱骂、敏感人物等。 异常链接检：赌博、色情、涉政、营销、游戏等 疑似隐私信息检测：身份证、电话、学生证、邮箱、内网ip等。 重大表述问题检测：国家领导及其重点思想、国家政策方针、党及民族等意识形态类问题。 我公司所提供的预检检测能力将通过集成方式将在线预检能力集成进学校网站群平台的系统内，避免二次登录，使站群各类型管理员进行安全检测方便快捷易用。 2、内容安全扫描服务 我公司所提供的内容安全扫描服务以机器+人工的双重检测模式，针对学校所有网站站点内容进行全面深度检测，及时发现问题整改。通过建立常态化检测机制，制定全量及增量检测策略，确保在动态网络环境中发现潜在内容安全问题，及时处置防护。 我公司所提供的内容安全扫描服务，支持扫描可通过自定义词库进行检测，扫描后进行智能+人工		
3	售后服务保障	具体要求		项	1

			双确认处置，形成详细报表报告，报告包括时间、字段、威胁等级、处理建议等信息。 我公司所提供的内容安全扫描范围包括涉政敏感词、黑链、暗链等内容，扫描完成后由人工审核核验后输出内容安全扫描服务报告。所提供的敏感词检测词库包含落马贪官、校内敏感词、隐私信息、恐爆违禁、政治敏感、色情低俗、重大表述问题、自定义词库等敏感内容信息。所提供的非法链接检测内容包括暗链、黑链、色情广告、黄赌毒、小说漫画、商业广告等非法链接及内容。 我公司所提供基础扫描服务，提供每月定期升级词库。采用机器+人工的双重检测，扫描完成后，由人工审核核验后输出分析报告，输出便于网站内容管理员整改的风险清单。 我公司所提供的网站敏感词扫描，针对所有网站页面完整采集扫描，以机器+人工的双重检测模式全面筛查敏感词，解决网站存量问题。针对增量页面定期采集，及时发现新问题并预警，及时发现新增网站敏感词问题。 我公司所提供网站非法链接扫描，针对网站中所有外部链接全部采集，以机器+人工双重检测模式逐条排查，全面规避色情/赌博/小说漫画/商业广告等非法外链风险。针对增量页面定期采集，及时抓取页面中新增的链接，精准识别非法链接。 我公司提供历史数据长期补扫服务，提供紧急敏感词提供周维度更新，普通敏感词提供月度更新。更新后对之前节点交付的历史数据进行补扫，同时提供长期的免费升级服务，确保站群平台内容安全的准确性和完整性。 我公司提供专有词库定制扫描服务，在标准化词库基础上，为学校提供私有化敏感词库的新增与维护能力，包括落马人员、校内领导、校训等。 我公司提供每年两次内容安全紧急事件的应急处置服务。 我公司提供每年3次对网站群站点全部网页和上传在网站上的附件(WORD、EXCEL、PPT、PDF)进行敏感词、非法链接等内容安全的全量扫描。 我公司提供每年9次对增量网页及附件进行敏感词、非法链接等内容安全的增量扫描。 3、响应支持服务 我公司提供 7*24 小时技术支持服务：提供 7 天×24 小时×365 天的电话支持服务，包括节假日，非工作时间均可通过电话进行各类常见问题疑难解答，问题咨询，产品使用指导等。 支持平台系统管理及网站管理员 1 人。	
--	--	--	--	--

			支持针对产品 bug 及时修复。 我公司提供平台故障诊断服务，当系统出现故障无法使用时，由工程师介入诊断问题点，并提出修复方案。 我公司提供远程操作支持服务，当进行疑难问题解答、问题咨询等服务时，可通过线上远程软件进行辅助，对校方进行一对一操作解答服务。 我公司提供安全漏洞修复，对安全厂商、上级部门的漏扫报告进行一对一资深技术分析、处理，提供书面的正式处理回复报告。 我公司提供平台故障修复服务，对平台在运行过程中出现的故障进行修复服务，确保平台稳定，正常运行。 4、我公司面向学校网站群负责部门提供专属网站实施设计服务： 我公司提供校领导简介网页维护服务，对校领导等重要页面进行协助维护服务，包括文章格式调整等服务。 我公司提供装饰图片制作服务，网站日常使用的装饰图片制作 10 张。 我公司提供栏目调整服务，根据客户要求对网站栏目框架进行调整。 我公司提供页面兼容性优化服务，当页面出现变形等视觉差异问题时，确保页面在主流浏览器版本下正常显示。 我公司提供模板调整服务，可在节假日，学校活动日等，对网站页面进行微调服务，链接、备案信息发生变化时进行网站页面处理。 5、例行检查服务 我公司提供例行检查服务包括站群保养服务 2 次/年，对站群环境进行保养，检查用户信息，及时禁用长期未登录或简单密码的账号，系统在长期运行后产生的垃圾文件清理，对系统中的安全配置、常见问题进行全面排查并优化，确保系统处于最优状态运行等。 我公司提供例行检查服务包括平台巡检 4 次/年，对网站群应用环境，进行全面检查、对各项日志进行人工分析，及时发现各项隐患，并生成巡检记录报告。 我公司提供例行检查服务包括安全补丁更新服务，更新网站群相关的安全补丁，同时对平台基础软件 Apache、tomcat 及 postgresql 进行配置优化及版本升级，检查历史安全补丁是否有遗漏，确保系
--	--	--	--

		统安全性。	
		6、安全服务支持：	
		我公司提供数据安全服务，当数据意外损坏或丢失，乙方使用现存的数据备份进行技术恢复，保证损失最小化。	
		我公司提供等保支持，在等级保护期间提供技术支持服务，包括但不限于对应应用安全配置整改等服务。	
		我公司提供攻防演练支持，提供攻防演练标准方案，配合学校进行演练前安全检查，当出现紧急情况时，提供应急团队紧急支持。	
		我公司提供专职服务，具有资深服务人员一对一服务于重要站点网站管理员（包含 100 个重要站点），提供重要院系/学院/部门网站管理员咨询，维护，远程技术指导服务。	
		7、售后质保服务时间要求：	
		(1) 我公司提供 3 年售后质保服务保障。	

附件 2:

供货内容及分项价格表

单位: 元

序号	供货内容类别	子系统/功能模块名称	产品名称及型号	制造厂(商)	单位	数量	单价	合价	质保期	备注
1	总体技术要求	基本要求	/	西安博达软件股份有限公司	/	/	/	/	三年	是否免税: 否
2	博达高校全媒体群管理平台软件 V2.0	网站群管理	博达高校全媒体群管理平台软件 V2.0	西安博达软件股份有限公司	套	1	214500.00	214500.00	三年	是否免税: 否
		网站建设								
		内容管理								
		统计分析								
		安全防护								
		安全中心								
3	售后服务保障	内容安全管理	/	西安博达软件股份有限公司	项	1	132300.00	132300.00	三年	是否免税: 否
		具体要求								

附件 3:

郑州大学信息系统建设网络安全责任协议

甲方: 郑州大学信息化办公室

乙方: 西安博达软件股份有限公司

甲、乙双方现就 郑州大学信息化办公室、网络管理中心郑州大学网站群平台安全升级采购项目 (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, 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，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）： 郑州大学信息化办公室 乙方（盖章）： 西安博达软件股份有限公司

部门负责人（签字）  法人或授权代表（签字）： 

签字日期：2022 年 12 月 26 日 签字日期：2022 年 12 月 15 日

附件 4:

郑州大学信息系统建设信息安全保密协议

甲方: 郑州大学信息化办公室

乙方: 西安博达软件股份有限公司

甲、乙双方现就 郑州大学信息化办公室、网络管理中心郑州大学网站群平台安全升级采购项目 (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。

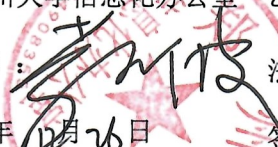
第十一条 乙方同意：若违反本协议内容，甲方有权制止乙方行为并要求其消除影响，视行为严重程度进行处罚；后果严重者，甲方将通过法律途径要求乙方进行经济赔偿，并向司法机关报案处理。

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）： 郑州大学信息化办公室 乙方（盖章）： 西安博达软件股份有限公司

部门负责人（签字）：  法人或授权代表（签字）： 

签字日期：2022年12月26日 签字日期：2022年12月15日

中标通知书

中 标 (成 交) 通 知 书

西安博达软件股份有限公司:

你方递交的郑州大学信息化办公室、网络管理中心郑州大学网站群平台安全升级采购项目投标文件,经专家评标委员会(或询价小组、竞争性磋商小组、竞争性谈判小组)评审,被确定为中标人。

主要内容如下:

项目名称	郑州大学信息化办公室、网络管理中心郑州大学网站群平台安全升级采购项目
采购编号	郑大-竞谈-2022-0059
中标(成交)价	346800元(人民币) 叁拾肆万陆仟捌佰元整(人民币)
供货期(完工期、服务期限)	10日历天
供货(施工、服务)质量	符合采购人要求
交货(施工、服务)地点	郑州大学
质保期	三年

请你方自中标通知书发出之日起3日内与招标人洽谈合同事项。联系人及电话:毛保磊 18729517229

特此通知。

采购单位(盖章)

代理单位(盖章)

2022年12月9日

中标单位签收人: 严亚朋

15840009664