合同编号：

郑州大学信息化办公室、网络管理中心

校园网网络安全保障与服务能力提升

（2026 年度）项目

服务合同

甲　方（全称）：郑州大学

乙　方（全称）：奇安信网神信息技术（北京）股份有限公司

依照《中华人民共和国民法典》及有关法律规定，遵循平等、自愿、公平和诚实信用的原则，甲乙双方就本服务采购相关事项协商一致，共同达成如下协议：

一、合同内容及要求：

校园网网络安全保障与服务能力提升（2026 年度）服务项目内容：

1、驻场服务。提供不少于 2 名专业驻场安全运营人员，服务期 6 个月，并提供二线专家团队 7×24 小时技术支撑服务；攻防演练及重保期间，乙方可根据学校实际需要增派驻场人员。驻场人员须严格执行学校相关考勤管理要求，落实上下班现场签到制度，每日做好出勤记录，服务期间输出《运营工作日报》《运管工作月报》《运营工作年报》《考勤表》等并统一归档留存。乙方对学校网络安全承担兜底责任，具体按本合同第十条约定执行。

2、资产管理与漏洞治理服务。协助学校完成信息资产管理工作，依托学校安全运营平台，对学校指定 IP 地址范围内的资产开展常态化管理，维护校园网资产台账并持续更新；对学校现有资产管理平台工具提供定制化升级，并与学校

现有态势感知平台实时同步资产信息。服务期间协助学校开展信息资产漏洞扫描、重点业务系统渗透检测，并为新上线系统提供源代码审计服务，免费提供商用源代码安全检测工具。

3、安全监测与日志分析服务。依托学校现有态势感知平台，由驻场人员持续对校园网威胁告警进行监测、研判、处置和事件调查，及时上报预警安全事件，实现安全事件闭环处理，输出《威胁监测日报》《威胁监测月报》《告警事件处置报告》等；驻场人员须熟练掌握学校现有态势感知平台的操作使用和运行维护，避免服务交接期出现防护空档。服务期间乙方在学校现有部署基础上，保障态势感知平台及流量探针、综合日志分析系统（不少于 200 点授权）授权有效并正常运行，规则库及威胁情报库在服务期内实时更新，对学校数据中心各类业务系统安全日志进行采集分析。

4、系统安全加固与终端防护服务。服务期间乙方为学校服务器安全加固系统更新授权（不少于 100 点授权），对学校重点服务系统提供安全加固服务；为学校现有终端安全防护管理系统提供 3000 点 1 年升级授权，并提供原厂授权书；对学校重点门户和业务网站提供 7×24 小时互联网监测服务，为互联网监测平台更新不少于 50 域名的 1 年使用授权。

5、配套服务与工具保障。服务期间乙方提供安全教育平台及安全技术实习生带训（20 人以内团队）、信息化专员和信息安全助理技术培训、网络安全宣传周活动支持、突发安全事件应急响应等服务；负责本项目服务工具与平台的授权更新、运维以及规则库、威胁情报库更新，服务工具与平台清单及授权数量以乙方响应文件为准，并作为项目初验的交付内容。

上述服务的具体技术参数、功能要求、服务频次及交付成果以本项目竞争性磋商文件和乙方响应文件为准。竞争性磋商文件、乙方响应文件及成交通知书作为本合同附件，与本合同具有同等法律效力；上述文件与本合同约定不一致的，以本合同约定为准。

二、合同总价款：

合同总价人民币 686,500.00 元，大写：陆拾捌万陆仟伍佰元整；其中不含税金额 647,641.51 元，税额 38,858.49 元（税率 6%）。

三、质量要求或服务标准，乙方对质量负责的条件和期限：

根据项目磋商文件及响应文件的服务要求，乙方提供不少于 2 名专业安全服务人员驻场，配合二线专家团队提供 7×24 小时技术支撑，为学校提供资产管理、漏洞治理、安全监测、日志分析、系统安全加固、互联网监测、重保值守、应急响应、安全教育培训及网络安全宣传等服务，并保障态势感知平台、流量探针、综合日志分析系统、服务器安全加固系统、互联网监测平台、安全教育平台等服务工具平台在服务期内的授权有效、正常运行。

服务期限为 6 个月。

四、服务约定：

1、服务完成时间：合同签订之日起 6 个月。

2、服务地点：甲方指定地点（郑州大学主校区）。

3、服务方式：现场驻场服务与远程支撑服务相结合。

五、验收标准、方法：（提供验收资料需一式三份）

1、验收标准

验收类别	要求指标	输出内容
服务授权更新	态势感知平台及流量探针、综合日志分析系统、服务器安全加固系统、互联网监测平台、安全教育平台、终端安全防护管理系统等，在学校现有部署基础上于初验之前完成授权续费及激活，全部达到授权有效、正常可用的状态，规则库、威胁情报库更新至最新；驻场人员到岗并完成进场手续，为学校网络安全提供支撑。	授权续费及激活确认单（或原厂授权书）、服务方案、工具与平台运行确认单、驻场人员到岗确认单
服务内容	资产梳理、业务中心网络拓扑梳理、漏洞扫描梳理、安全策略梳理、服务器加固服务、日常监测分析报告、重保值守报告、应急响应服务报告、漏洞通报服务等；完成资产信息台账（基线版）及服务期工作计划。	保密协议、对应的文档模板
项目总结与归档	各类项目过程文档和工作成果交付文档，归档的文件清单，项目整体工作实施情况等。	各类项目文档报告，项目文档清单，项目总结报告
项目验收	项目验收意见。	经评审和确认的项目验收报告

六、结算方式及期限：

验收合格并经审计后付合同总金额的95%，余款在质保期满后结清。

七、免费质保约定：

乙方应确保服务期间服务工具与平台处于有效授权和版本最新状态，规则库、威胁情报库实时更新；如服务工具出现硬件故障等，由乙方负责协调维修，并提供备用产品。质保期为服务期满后 3 个月，质保期内乙方免费提供远程技术支持，并对服务质量问题免费整改。

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）

服务内容：（同本合同内容及要求）

服务方式：现场服务结合远程服务

响应时间：随时响应

服务电话：95015、17760777519

服务期限：合同签订之日起6个月

质保期满结束后的维保：服务期满后如需继续提供维保服务，由双方另行协商。

九、履约担保

合同总价款10万元（含10万元）至100万元（不含100万元）不强制提供保函或现金履约担保，由甲方和乙方双方协商；合同总价款100万元以上（含100万元）的履约担保金额为合同总额的5%，履约担保方式为：乙方以银行保函方式在合同签订前向甲方提供履约担保，验收合格、正式交付使用后退还。

本合同总价款为686,500.00元，处于10万元（含）至100万元（不含）区间，经双方协商，本项目不提供履约担保。

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或服务标准，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，乙方还应按给甲方造成的经济损失赔偿；乙方未按约定期限提供服务，每迟延一天须按合同总价款的1%向甲方支付违约金。如果乙方对合同迟延履行超过合理期限，甲方有权解除或终止合同，并且要求乙方赔偿由此给甲方造成的经济损失。

乙方对学校网络安全施行兜底责任制，即学校每收到1个国家级的网络安全方面的整改报告，扣除合同金额5万元；每收到1个省级的网络安全方面的整改报告，扣除合同金额2万元；每收到1个地市级的网络安全方面的整改报告，扣除合同金额1万元；因本合同第十二条第1款约定情形产生的整改报告，不适用本款扣款。

2、甲方违约：甲方未能按双方约定的方式和期限支付合同价款，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）：河南省郑州市郑东新区龙湖中环南路与如意西路交汇处龙湖国际中心北楼5层510，齐壮 18539941818。

十二、其它约定事项：

1、如在服务过程中，安全整改报告由以下原因导致，如甲方人员主观人为过失行为导致的安全事故或数据泄露；由自然灾害、战争、恐怖袭击或其他不可预见且不可避免的因素引起的，乙方可不承担责任，因上述情形产生的整改报告不适用本合同第十条约定的兜底扣款。

2、乙方应遵守《中华人民共和国网络安全法》等法律法规及学校网络安全管理规定，按本合同附件1承担网络安全责任、按附件2承担信息保密义务。

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 捌 份、副本 贰 份，甲方执 陆 份，乙方执 贰 份，报送招标代理机构 贰 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）：	乙方（盖章）：
法定代表人或授权代表：	法定代表人或授权代表：
单位地址：郑州市高新区科学大道 100 号	单位地址：北京市西城区西直门外南路 26 号院 1 号楼 2 层
电　　话：0371-67781507	电　　话：010-62972893
开户银行：工商银行郑州中苑名都支行	开户银行：招商银行北京建国路支行
户　　名：郑州大学	户　　名：奇安信网神信息技术（北京）股份有限公司
账　　号：1702021109014403854	账　　号：110902261210404
签订日期：2026 年 11 月 13 日	

签约地点：河南省郑州市高新区科学大道 100 号（郑州大学）

附件 1：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：奇安信网神信息技术（北京）股份有限公司

甲乙双方现就郑州大学信息化办公室、网络管理中心校园网网络安全保障与服务能力提升（2026 年度）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、售后服务和后续合作过程中，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。

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）：		乙方（盖章）：
部门负责人（签字）：		法定代表人或授权代表（签字）：
签字日期：2021 年 4 月 13 日		

附件 2：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：奇安信网神信息技术（北京）股份有限公司

甲乙双方现就郑州大学信息化办公室、网络管理中心校园网网络安全保障与服务能力提升（2026 年度）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、售后服务和后续合作过程中，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。

第三条　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，亦属于本协议约定的保密信息。

第四条　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。

第五条　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。

第六条 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。

第七条 乙方应采取必要措施保护和妥善保存从甲方获取的保密信息，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。

第八条 乙方不得刺探与本项目无关的甲方保密信息。

第九条 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。

第十条 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。

第十一条 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。

第十二条 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。

第十三条 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。

第十四条 乙方的保密义务自本协议盖章之日起开始生效。

第十五条 乙方的保密义务并不因双方合作关系的解除而免除。

第十六条 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）：		乙方（盖章）：	
部门负责人（签字）：		法定代表人或授权代表（签字）：	
签字日期： 2026年11月13日			

合同编号：

郑州大学信息化办公室、网络管理中心

校园网网络安全保障与服务能力提升

（2026 年度）项目

服务合同

甲　方（全称）：郑州大学

乙　方（全称）：奇安信网神信息技术（北京）股份有限公司

依照《中华人民共和国民法典》及有关法律规定，遵循平等、自愿、公平和诚实信用的原则，甲乙双方就本服务采购相关事项协商一致，共同达成如下协议：

一、合同内容及要求：

校园网网络安全保障与服务能力提升（2026 年度）服务项目内容：

1、驻场服务。提供不少于 2 名专业驻场安全运营人员，服务期 6 个月，并提供二线专家团队 7×24 小时技术支撑服务；攻防演练及重保期间，乙方可根据学校实际需要增派驻场人员。驻场人员须严格执行学校相关考勤管理要求，落实上下班现场签到制度，每日做好出勤记录，服务期间输出《运营工作日报》《运管工作月报》《运营工作年报》《考勤表》等并统一归档留存。乙方对学校网络安全承担兜底责任，具体按本合同第十条约定执行。

2、资产管理与漏洞治理服务。协助学校完成信息资产管理工作，依托学校安全运营平台，对学校指定 IP 地址范围内的资产开展常态化管理，维护校园网资产台账并持续更新；对学校现有资产管理平台工具提供定制化升级，并与学校

现有态势感知平台实时同步资产信息。服务期间协助学校开展信息资产漏洞扫描、重点业务系统渗透检测，并为新上线系统提供源代码审计服务，免费提供商用源代码安全检测工具。

3、安全监测与日志分析服务。依托学校现有态势感知平台，由驻场人员持续对校园网威胁告警进行监测、研判、处置和事件调查，及时上报预警安全事件，实现安全事件闭环处理，输出《威胁监测日报》《威胁监测月报》《告警事件处置报告》等；驻场人员须熟练掌握学校现有态势感知平台的操作使用和运行维护，避免服务交接期出现防护空档。服务期间乙方在学校现有部署基础上，保障态势感知平台及流量探针、综合日志分析系统（不少于 200 点授权）授权有效并正常运行，规则库及威胁情报库在服务期内实时更新，对学校数据中心各类业务系统安全日志进行采集分析。

4、系统安全加固与终端防护服务。服务期间乙方为学校服务器安全加固系统更新授权（不少于 100 点授权），对学校重点服务系统提供安全加固服务；为学校现有终端安全防护管理系统提供 3000 点 1 年升级授权，并提供原厂授权书；对学校重点门户和业务网站提供 7×24 小时互联网监测服务，为互联网监测平台更新不少于 50 域名的 1 年使用授权。

5、配套服务与工具保障。服务期间乙方提供安全教育平台及安全技术实习生带训（20 人以内团队）、信息化专员和信息安全助理技术培训、网络安全宣传周活动支持、突发安全事件应急响应等服务；负责本项目服务工具与平台的授权更新、运维以及规则库、威胁情报库更新，服务工具与平台清单及授权数量以乙方响应文件为准，并作为项目初验的交付内容。

上述服务的具体技术参数、功能要求、服务频次及交付成果以本项目竞争性磋商文件和乙方响应文件为准。竞争性磋商文件、乙方响应文件及成交通知书作为本合同附件，与本合同具有同等法律效力；上述文件与本合同约定不一致的，以本合同约定为准。

二、合同总价款：

合同总价人民币 686,500.00 元，大写：陆拾捌万陆仟伍佰元整；其中不含税金额 647,641.51 元，税额 38,858.49 元（税率 6%）。

三、质量要求或服务标准，乙方对质量负责的条件和期限：

根据项目磋商文件及响应文件的服务要求，乙方提供不少于 2 名专业安全服务人员驻场，配合二线专家团队提供 7×24 小时技术支撑，为学校提供资产管理、漏洞治理、安全监测、日志分析、系统安全加固、互联网监测、重保值守、应急响应、安全教育培训及网络安全宣传等服务，并保障态势感知平台、流量探针、综合日志分析系统、服务器安全加固系统、互联网监测平台、安全教育平台等服务工具平台在服务期内的授权有效、正常运行。

服务期限为 6 个月。

四、服务约定：

1、服务完成时间：合同签订之日起 6 个月。

2、服务地点：甲方指定地点（郑州大学主校区）。

3、服务方式：现场驻场服务与远程支撑服务相结合。

五、验收标准、方法：（提供验收资料需一式三份）

1、验收标准

验收类别	要求指标	输出内容
服务授权更新	态势感知平台及流量探针、综合日志分析系统、服务器安全加固系统、互联网监测平台、安全教育平台、终端安全防护管理系统等，在学校现有部署基础上于初验之前完成授权续费及激活，全部达到授权有效、正常可用的状态，规则库、威胁情报库更新至最新；驻场人员到岗并完成进场手续，为学校网络安全提供支撑。	授权续费及激活确认单（或原厂授权书）、服务方案、工具与平台运行确认单、驻场人员到岗确认单
服务内容	资产梳理、业务中心网络拓扑梳理、漏洞扫描梳理、安全策略梳理、服务器加固服务、日常监测分析报告、重保值守报告、应急响应服务报告、漏洞通报服务等；完成资产信息台账（基线版）及服务期工作计划。	保密协议、对应的文档模板
项目总结与归档	各类项目过程文档和工作成果交付文档，归档的文件清单，项目整体工作实施情况等。	各类项目文档报告，项目文档清单，项目总结报告
项目验收	项目验收意见。	经评审和确认的项目验收报告

六、结算方式及期限：

验收合格并经审计后付合同总金额的95%，余款在质保期满后结清。

七、免费质保约定：

乙方应确保服务期间服务工具与平台处于有效授权和版本最新状态，规则库、威胁情报库实时更新；如服务工具出现硬件故障等，由乙方负责协调维修，并提供备用产品。质保期为服务期满后 3 个月，质保期内乙方免费提供远程技术支持，并对服务质量问题免费整改。

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）

服务内容：（同本合同内容及要求）

服务方式：现场服务结合远程服务

响应时间：随时响应

服务电话：95015、17760777519

服务期限：合同签订之日起6个月

质保期满结束后的维保：服务期满后如需继续提供维保服务，由双方另行协商。

九、履约担保

合同总价款10万元（含10万元）至100万元（不含100万元）不强制提供保函或现金履约担保，由甲方和乙方双方协商；合同总价款100万元以上（含100万元）的履约担保金额为合同总额的5%，履约担保方式为：乙方以银行保函方式在合同签订前向甲方提供履约担保，验收合格、正式交付使用后退还。

本合同总价款为686,500.00元，处于10万元（含）至100万元（不含）区间，经双方协商，本项目不提供履约担保。

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或服务标准，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，乙方还应按给甲方造成的经济损失赔偿；乙方未按约定期限提供服务，每迟延一天须按合同总价款的1%向甲方支付违约金。如果乙方对合同迟延履行超过合理期限，甲方有权解除或终止合同，并且要求乙方赔偿由此给甲方造成的经济损失。

乙方对学校网络安全施行兜底责任制，即学校每收到1个国家级的网络安全方面的整改报告，扣除合同金额5万元；每收到1个省级的网络安全方面的整改报告，扣除合同金额2万元；每收到1个地市级的网络安全方面的整改报告，扣除合同金额1万元；因本合同第十二条第1款约定情形产生的整改报告，不适用本款扣款。

2、甲方违约：甲方未能按双方约定的方式和期限支付合同价款，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）：河南省郑州市郑东新区龙湖中环南路与如意西路交汇处龙湖国际中心北楼5层510，齐壮 18539941818。

十二、其它约定事项：

1、如在服务过程中，安全整改报告由以下原因导致，如甲方人员主观人为过失行为导致的安全事故或数据泄露；由自然灾害、战争、恐怖袭击或其他不可预见且不可避免的因素引起的，乙方可不承担责任，因上述情形产生的整改报告不适用本合同第十条约定的兜底扣款。

2、乙方应遵守《中华人民共和国网络安全法》等法律法规及学校网络安全管理规定，按本合同附件1承担网络安全责任、按附件2承担信息保密义务。

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 捌 份、副本 贰 份，甲方执 陆 份，乙方执 贰 份，报送招标代理机构 贰 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）：	乙方（盖章）：
法定代表人或授权代表：	法定代表人或授权代表：
单位地址：郑州市高新区科学大道 100 号	单位地址：北京市西城区西直门外南路 26 号院 1 号楼 2 层
电　　话：0371-67781507	电　　话：010-62972893
开户银行：工商银行郑州中苑名都支行	开户银行：招商银行北京建国路支行
户　　名：郑州大学	户　　名：奇安信网神信息技术（北京）股份有限公司
账　　号：1702021109014403854	账　　号：110902261210404
签订日期：2026 年 11 月 13 日	

签约地点：河南省郑州市高新区科学大道 100 号（郑州大学）

附件 1：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：奇安信网神信息技术（北京）股份有限公司

甲乙双方现就郑州大学信息化办公室、网络管理中心校园网网络安全保障与服务能力提升（2026 年度）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、售后服务和后续合作过程中，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。

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）：	乙方（盖章）：
部门负责人（签字）：	法定代表人或授权代表（签字）：
签字日期：2021 年 11 月 13 日	

附件 2：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：奇安信网神信息技术（北京）股份有限公司

甲乙双方现就郑州大学信息化办公室、网络管理中心校园网网络安全保障与服务能力提升（2026 年度）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、售后服务和后续合作过程中，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。

第三条　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，亦属于本协议约定的保密信息。

第四条　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。

第五条　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。

第六条 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。

第七条 乙方应采取必要措施保护和妥善保存从甲方获取的保密信息，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。

第八条 乙方不得刺探与本项目无关的甲方保密信息。

第九条 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。

第十条 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。

第十一条 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。

第十二条 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。

第十三条 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。

第十四条 乙方的保密义务自本协议盖章之日起开始生效。

第十五条 乙方的保密义务并不因双方合作关系的解除而免除。

第十六条 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）：	乙方（盖章）：
部门负责人（签字）：	法定代表人或授权代表（签字）：
签字日期：2026年1月13日	