合同编号：_____

郑州大学继续教育学院远程教育学院网络安全服务采购合同

甲方（全称）：郑州大学

乙方（全称）：河南金盾信安检测评估中心有限公司

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：

（一）网络安全运维服务

服务期内提供安全运维服务，在服务期内应根据甲方运维和等级保护需求，对在线教育综合服务平台系统范围内的子应用模块，开展不定期、不限次数的网络安全漏洞检查，同时配套提供等级保护基础巡检、安全巡检、安全扫描、漏洞通告、日志分析、应急响应等日常安全运营、运维服务工作，提升系统的动态安全防御能力。

1.1 基础巡检服务

依据国家等级保护建设技术标准，结合我院目前网络拓扑结构，要求服务方对我院数据中心机房内运行维护范围内的 IT 资产进行梳理，包括现有设备硬件及软件资产，按照动力环境、服务器类、网络设备类、网络安全设备类等分类建立相应的巡检计划，巡检应包括巡检内容、巡检周期、巡检报告以及问题处理建议等。

1.2 安全巡检服务

安全巡检服务应区别于基础巡检服务，要求对我院数据中心的整体安全状况进行分析和评估，对我院信息系统的安全配置进行检查，要求应能通过安全巡检服务发现安全风险并及时提出整改措施，协助我院进行安全加固。

1.3 运维监控系统搭建及运维

通过此服务实现监控服务器硬件；监控主机 CPU/内存/硬盘/网络吞吐；监控核心交换、接入交换等网络设备及安全设备运行状态以及生成网络拓扑，进行报警提醒。

1.4 安全应急响应

应急响应服务是应对我院紧急安全事件时服务方提供的技术服务，要求对我院技术人员无法迅速解决的网络入侵、拒绝服务攻击、大规模病毒爆发、主机或网络异常事件等紧急安全问题提供技术支持，控制事态发展；保护或恢复我院主机、网络服务的正常工作；并且提供事后分析，找出我院系统的安全漏洞，根据现场保留数据痕迹情况协助我院对入侵者进行追查。紧急响应服务方式应包括远程支持和现场支持，远程支持应采用电话、远程加密登录等手段。当远程支持无法解决问题时，根据事件时间紧急程度以及我院的要求，服务方应派遣专业的紧急响应服务人员在第一时间到达我院所在地提供现场服务。

1.5 安全漏洞扫描

服务方应通过安全工具对网络设备、安全设备、主机、数据库、应用等对象进行检查和分析，应包含但不限于：安全扫描（系统扫描和应用扫描）、本地后门排查、基线检查和安全日志审计等内容。

1.6 安全通告服务

服务方技术团队应不定期以安全通告的形式为我院提供最新的安全动态、技术和定制的安全信息，包括实时安全漏洞通知、病毒、补丁升级、定期安全知识库更新等，特别是高危漏洞出现和发布后，服务方安服团队应在第一时间根据我院系统情况有针对性地提供漏洞预警、安全加固建议，并提供漏洞验证和复现的测试协助。

1.7 渗透测试服务

根据我院的网络安全具体需求，要求服务方采用人工渗透的方式来评估我院系统的安全性。服务范围应包括我院对外提供访问服务的网站、网络及其他应用系统，涵盖漏洞分析及渗透模拟入侵测试等安全评估形式。

1.8 入网设备安全配置加固服务

针对运维期内我院新入网的安全设备、服务器、应用系统，服务方应提供安全配置的加固，保证新入网的安全设备符合我院整体安全策略，降低新入网设备可能引入的新安全风险。

1.9 安全培训服务

为了提升我院的安全管理素养，使我院技术人员能够具备应用系统工程安全运维管理的能力，服务方应提供关于等级保护相关的技术培训，以满足我院不同时期的需求。

1.10 设备利旧服务

要求服务方对我院内部未启用的相关设备进行合理利用，根据我院实际设备情况，结合我院网路拓扑结构，通过配置达到合理化设备利旧，优化和节约资金。

(二) 网络安全等级保护安全建设服务

服务期内对服务范围清单（项目服务范围：在线教育服务平台应用系统、平台运行虚拟机、物理服务器、存储设备、交换机、防火墙、审计系统等相关安全软硬件）中的所有设备及服务器上运行的虚拟系统开展网络安全等级保护安全建设服务，按照国家等级保护 2.0 二级信息系统技术标准进行，通过此项服务完善系统安全顶层设计并调优网络架构，搭建符合等级保护要求的网络安全防护体系，通过此次等级保护安全建设服务提升网络安全防护能力，确保顺利通过系统等级保护二级测评。

2.1 新入网安全服务工具集成及部署服务

在服务期内，服务方应依据等级保护 2.0 设计和建设的相关技术标准，结合我院目前网络拓扑结构，对我院的网络安全技术服务工具进行科学的合规性设计与部署适配交付，在安全集成与交付过程当中，服务方应确保设备的策略配置符合等级保护要求，实现业务系统及网络在最小停机时间内的平滑、稳定升级。

2.2 核心区域网络设计与划分

服务方应结合安全重要等级对核心区域进行合理规划和分区设计，最后依据等级保护分区分域原则和设计规划，实现核心区域划分并整理归纳出《安全策略梳理表》，现有安全策略存在不合理的地方需要通过本次服务对安全策略进行修订、加固或者策略重建，网络架构存在不合理的地方需要重新调整网络架构实现策略落地。

2.3 外联区域划分

服务方应根据我院业务实际需求和等级保护技术要求，通过边界隔离设备的有效结合，在拓扑逻辑结构上构造出外联区域，将外联区域与其他互联区域进行边界划分，配置外联区域防火墙、内网边界的进站、出站访问控制策略，完成对

通过边界设备的应用数据流进行梳理和应用端口识别，达到安全策略精度到端口级，施工完成后应提交区域间策略设置文档。

2.4 防火墙访问控制策略梳理与加固服务

要求服务方对我院现有的边界防火墙访问控制策略进行梳理及加固，因等级保护建设的核心就是分区分域，而防火墙作为边界设备及安全策略管控的有效载体，在整个等级保护安全建设当中处于关键核心位置，边界防火墙安全策略的配置的合理和严谨性代表了网络抵御风险和抗攻击能力的高低，因此要求服务方在本项目中将防火墙访问控制策略梳理与加固服务作为一项重要的服务内容进行规划和明确。

2.5 补丁升级服务

要求本次项目的服务方将对全网所有使用微软操作系统的服务器进行安全补丁升级加固，搭建微软官方补丁安全升级服务器，为全网所有 windows 终端提供升级服务；在加固过程中提供数据库、中间件以及 linux 系统补丁升级咨询建议，配合我院对以上存在漏洞的系统组件进行安全版本升级测试服务，配合测试完成后提供相应安全测试或者加固服务报告。

2.6 主机加固服务

按照等级保护技术要求，要求服务方针对系统账户安全，依据最小化服务原则，对访问控制策略配置，用户鉴别、审计策略等内容进行安全整改及加固。服务对象包含本次等级保护系统所包含的所有服务器。

2.7 网络设备加固服务

网络设备加固应包括本次项目实施阶段的阶段性安全加固和后期运维阶段的网络加固，项目实施期间的安全加固主要是网络设备架构调整以及设备内部策略配置，加固之后符合等级保护要求，在安全域划分基础上，构建整体网络安全立体防护体系。运维阶段的服务主要是根据我院业务需求的变化调整网络架构和策略设置，保证网络设备的策略配置持续更新。

2.8 日志回溯与分析服务

此项服务主要是结合本次服务中服务方提供的安全集中管控平台工具，收集安全日志，进行事件审计和日志分析，对安全策略进行有效性验证，检查策略是否有效，配置是否安全，是否有可疑事件发生，据此进行边界安全设备、网络设备、应用防护系统安全策略的调整。

2.9 漏洞扫描服务

项目安服人员基于漏洞数据库，通过扫描等手段对段对指定的系统的进行安全脆弱性检测。利用扫描检测类的专业工具对我院的主机、网络、应用、数据库以及数据库中间件等层面进行工具类的批量化扫描，做系统安全层面的覆盖性检测，补充人工渗透发现漏洞的种类和数量，此外利用工具提升漏洞发现的效率；

2.10 安全管理制度设计

要求服务方根据等级保护基本要求、安全需求分析报告、我院总体安全策略文件等安全管理体系建设内容，协助我院从全局高度考虑制定统一的安全管理策略，选择和调整具体的安全管理措施，最后形成统一的整体安全管理体系结构，具体包括但不限于以下内容：

规定信息安全的组织管理体系和对各信息系统的安全管理职责。

规定各等级信息系统的人员安全管理策略。

规定各等级信息系统机房及办公区等物理环境的安全管理策略。

规定各等级信息系统介质、设备等的安全管理策略。

规定各等级信息系统运行安全管理策略。

规定各等级信息系统安全事件处置和应急管理策略。

要求服务方由以上文档形成信息系统安全管理策略框架。

(三) 网络安全等级保护测评服务

1、完成甲方在线教育综合服务平台系统的二级等级保护测评工作。

2、负责整个测评过程中的技术对接，针对提出的不符合项、部分符合项进行技术确认和答复，并协助甲方完成技术性安全加固整改，保障甲方的相关的测评权益不受影响，最大化地提升测评最终得分，协助完成在线教育服务平台在当地网安部门的网络安全等级保护备案工作。

二、合同总价款：

本合同总金额为￥115,000.00 元（大写：人民币壹拾壹万伍仟元整），其中不含增值税的金额为￥108,490.57 元，增值税预估税额为￥6,509.43 元，增值税税率为 6%。

三、质量要求或服务标准，乙方对质量负责的条件和期限：

1. 乙方严格按照国家标准进行网络安全等级保护测评等网络安全服务工作。

2. 乙方严格遵守保密协议中的相关约定，做好双方信息的保密工作。

3. 乙方在甲方指定的地点开展测评及网络安全服务工作。

4. 乙方指派工作经验丰富的项目经理，结合技术领先、结论可靠的测评及网络安全服务工具为甲方做全面的安全测评及网络安全服务。

5. 乙方按照标准性、规范性、可控性、整体性、最小影响性及保密性的原则指导下，开展等测评及网络安全服务工作，做到守时保质。

6. 乙方在实施关键网络安全服务项时（如漏洞扫描或工具测试等），要与甲方充分沟通该关键项实施的细节与步骤，得到甲方许可后，再开展该项安全服务，以安全服务项对甲方的信息系统影响最小化为目标。

四、服务约定：

1、服务完成时间：签订合同后365日历天内完成项目。

2、服务地点：甲方指定地点。

3、服务方式：现场测评。

五、验收标准、方法：（需提供三份验收资料）

1.乙方应向甲方提供本合同项下的技术资料或成果。技术资料的费用应包括在合同总金额中。

2.本合同项下的技术资料和成果为1、《信息系统基本情况调查表》《网络安全等级保护测评报告》；2、《信息系统漏洞扫描报告》《信息系统渗透测试报告》《信息系统网站渗透测试复测报告》《漏洞通告报告》《相关管理制度》；3、《整改建议方案》。

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30天内结清。

七、免费质保约定：

免费质保期为一年，质保期内免费提供信息安全咨询工作，免费提供本项目合同范围内的信息系统上线前安全检测服务。

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、乙方对所测试的信息系统（网站）提供为期一年的售后服务，包括问题排查、漏洞修复、系统加固、应急处置等。

2、在售后服务期限内，乙方免费提供技术维护及现场技术支持，且所使用的任何相关工具必须经用户认可。

九、履约担保

乙方提供履约担保的形式：以转账的方式提供；

履约担保金额：合同总价款的 5%；

履约担保期限：1 年；履约担保的有效期始于工程开工之日，终止日期则可以约定为工程竣工交付之日。履约担保金在签订合同前交学校财务处，工程竣工验收合格交付使用后履行手续退还。

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；乙方未按约定期限交付标的物，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。

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）：郑州市郑东新区中道东路 6 号创意岛大厦 B 区 B620。

十二、 其它约定事项：

无

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，甲方执陆份，乙方执贰份，具有同等法律效力。

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：郑州大学

电话：6776322

开户银行：工商银行郑州中原名都支行

户名：郑州大学

帐号：1702021109014403854

签定日期：2023.3.16

乙方（盖章）：河南金盾信安检测评估中心有限公司

法定代表或代理人：

单位地址：郑州市郑东新区中道东路 6 号创意岛大厦 B 区 B620

电话：0371-55395206

开户银行：上海浦东发展银行郑州经三路支行

户名：河南金盾信安检测评估中心有限公司

帐号：76060154800006231

签定日期：2023.3.16

签约地点：河南省郑州市

中 标（成交）通 知 书

河南金盾信安检测评估中心有限公司：

你方递交的郑州大学继续教育学院远程教育学院网络安全服务项目投标文件，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	郑州大学继续教育学院远程教育学院网络安全服务项目
采购编号	郑大-竞磋-2022-0068
中标（成交） 价	115000 元(人民币) 壹拾壹万伍仟元整(人民币)
供货期（完工期、服务期限）	签订合同后 365 个日历天
供货（施工、服务）质量	合格，满足采购需求
交货（施工、服务）地点	采购人指定地点

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：赵红领 18530017788

特此通知。

采购单位(盖章)　　代理单位（盖章）

2022 年 12 月 5 日

中标单位签收人：

史[illegible]，13849860922

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： 河南金盾信安检测评估中心有限公司

甲、乙双方现就 郑州大学继续教育学院远程教育学院网络安全服务项目（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 本协议一式陆份，甲方执肆份，乙方执贰份，具有同等法律效力。

甲方（盖章）： 郑州大学

部门负责人（签字）：

签字日期：2023.3.16

乙方（盖章）：河南金盾信安检测评估中心有限公司

法人或授权代表（签字）：

签字日期：2023.3.16

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：河南金盾信安检测评估中心有限公司

甲、乙双方现就郑州大学继续教育学院远程教育学院网络安全服务项目（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 本协议一式陆份，甲方执肆份，乙方执贰份，具有同等法律效力。

甲方（盖章）： 郑州大学

部门负责人（签字）：

签字日期：2023.3.16

乙方（盖章）：河南金盾信安检测评估中心有限公司

法人或授权代表（签字）：

签字日期：2023.3.16

附件 3

网络安全运维服务协议

甲方：郑州大学

乙方：河南金盾信安检测评估中心有限公司

一、协议内容及要求：

序号	技术分类	安全检测服务技术规格参数、功能描述
1	需遵循的标准、指南或规范	依据 ISO/IEC 27001:2005 信息技术-安全技术-信息系统规范与使用指南
		依据 ISO/IEC 13335-1:2004 信息技术-安全技术-信息技术安全管理指南
		依据 ISO/IEC TR 15443-1:2005 信息技术安全保障框架
		依据 ISO/IEC PDTR 19791:2004 信息技术 安全技术 运行系统安全评估
		依据 GB/T 20984-2007 信息安全技术 信息安全风险评估规范
		依据 GB/T 19715.1-2005 信息技术-信息技术安全管理指南
		依据 GB/T 19716-2005 信息技术-信息安全管理实用规则
		依据 GB/T 18336-2001 信息技术-安全技术-信息技术安全性评估准则
		依据 GB/T17859-1999 计算机信息系统安全保护等级划分准则
		依据 GB/T 20984-2007 信息安全技术 信息安全风险评估规范
		依据 GB/T 20988-2007 信息系统灾难恢复规范
		依据 GB/Z 20986-2007 信息安全事件分类分级指南
		依据信息系统审计标准（ISACA）G3 利用计算机辅助审计技术
		依据信息系统审计标准（ISACA）G7 应有的职业谨慎
		依据信息系统审计标准（ISACA）G9 不正当行为的审计考虑
		依据信息系统审计标准（ISACA）G18 信息系统管理
		依据信息系统审计标准（ISACA）G19 不正当及非法行为
		依据信息系统审计标准（ISACA）G33 对网络使用的总体考虑
		依据 CESG（CHECK）IT Health Check 方法
		依据 OWASP OWASP_Testing_Guide_v3
		依据 OWASP OWASP_Development_Guide_2005
		依据 OWASP OWASP_Top_10_2010_Chinese_V1.0
		依据 OSSTMM OSSTMM_Web_App_Alpha
		依据 Web 应用安全委员会（WASC）WASC Threat Classification v2

附件 3

网络安全运维服务协议

甲方：郑州大学

乙方：河南金盾信安检测评估中心有限公司

一、协议内容及要求：

序号	技术分类	安全检测服务技术规格参数、功能描述
1	需遵循的标准、指南或规范	依据 ISO/IEC 27001:2005 信息技术-安全技术-信息系统规范与使用指南
		依据 ISO/IEC 13335-1:2004 信息技术-安全技术-信息技术安全管理指南
		依据 ISO/IEC TR 15443-1:2005 信息技术安全保障框架
		依据 ISO/IEC PDTR 19791:2004 信息技术 安全技术 运行系统安全评估
		依据 GB/T 20984-2007 信息安全技术 信息安全风险评估规范
		依据 GB/T 19715.1-2005 信息技术-信息技术安全管理指南
		依据 GB/T 19716-2005 信息技术-信息安全管理实用规则
		依据 GB/T 18336-2001 信息技术-安全技术-信息技术安全性评估准则
		依据 GB/T17859-1999 计算机信息系统安全保护等级划分准则
		依据 GB/T 20984-2007 信息安全技术 信息安全风险评估规范
		依据 GB/T 20988-2007 信息系统灾难恢复规范
		依据 GB/Z 20986-2007 信息安全事件分类分级指南
		依据信息系统审计标准（ISACA）G3 利用计算机辅助审计技术
		依据信息系统审计标准（ISACA）G7 应有的职业谨慎
		依据信息系统审计标准（ISACA）G9 不正当行为的审计考虑
		依据信息系统审计标准（ISACA）G18 信息系统管理
		依据信息系统审计标准（ISACA）G19 不正当及非法行为
		依据信息系统审计标准（ISACA）G33 对网络使用的总体考虑
		依据 CESG（CHECK）IT Health Check 方法
		依据 OWASP OWASP_Testing_Guide_v3
		依据 OWASP OWASP_Development_Guide_2005
		依据 OWASP OWASP_Top_10_2010_Chinese_V1.0
		依据 OSSTMM OSSTMM_Web_App_Alpha
		依据 Web 应用安全委员会（WASC）WASC Threat Classification v2

		应用系统	包括但不限于 Oracle、MySQL、MSSQL、Sybase、DB2、Informix 等主流数据库，Apache、IIS、Tomcat、Weblogic 等主流 WEB 服务器，FTP、DNS 等主流应用服务器。
		WEB 程序	包括但不限于 ASP、PHP、JSP、.NET、Perl、Python、Shell 等语言编写的 WEB 程序。
		网络设备	常见厂商的路由器、交换机等设备。
6	服务方式	现场检测。	
7	服务周期	1年。	
8	检测人员	5人。	
		所有检测人员具备相应的安全服务能力。	
9	服务方案	乙方提供完整的安全检测服务实施方案和测试流程，包括但不限于准备阶段、测试阶段、整改阶段、复测阶段、汇总阶段等。	
10	整改服务	乙方针对信息系统发现的安全问题和安全风险，出具信息系统渗透测试报告，并协助完成系统安全修复与加固，加固对象包括但不限于服务器操作系统、数据库、中间件软件、应用系统关键运行设备；加固完成后，我方对加固对象进行复测，并出具系统复测报告。	
11	交付成果	交付成果包括但不限于《信息系统渗透测试报告》、《信息系统网站渗透测试复测报告》、《漏洞通告报告》、《相关管理制度》等。	
		所有交付成果均由具备信息安全等级保护服务资质的机构盖章。	
12	测试方式	以人工测试为主，使用专用工具辅助。	
13	测试工具	已在实施方案中提供详细的测试工具清单。	
14	售后服务	乙方对所测试的信息系统安全性提供一年的售后服务。（包括但不限于问题排查、漏洞修复、系统加固、应急处置等）	
		7*24 无限次数上门服务，2 小时到达用户现场。	

二、质量要求或服务标准，乙方对质量负责的条件和期限：

乙方须按合同要求提供信息系统（网站）安全检测服务（包括所需的专业工具、人员等），服务的质量标准、具体要求等符合项目要求，且应达到乙方响应文件及澄清文件中明确的技术标准。在服务过程中，甲方有权采取适当的方式对乙方安全检测服务质量标准、具体要求以及服务进度进行检查。甲方如果发现乙方所提供的安全检测服务不符合合同约定，甲方有权单方解除合同，由此产生的一切费用由乙方承担。

通过乙方检测的信息系统，存在学校检测扫描并通报但乙方未能检测出的漏洞，每通报一个漏洞扣除乙方 500 元服务费，存在校外安全机构检测扫描并通报

但乙方未能检测出的漏洞，每通报一个漏洞扣除乙方1000元服务费。

三、服务约定：

1.服务完成时间： 签订合同后365日历天内完成项目 。

2.服务地点： 郑州大学继续教育学院 远程教育学院 。

3.服务方式： 现场测评 。

四、免费质保约定：

免费质保期为一年，质保期内免费提供信息安全咨询工作，免费提供本项目合同范围内的信息系统上线前安全检测服务。

五、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、乙方对所测试的信息系统（网站）提供为期一年的售后服务，包括问题排查、漏洞修复、系统加固、应急处置等。

2、在售后服务期限内，乙方免费提供技术维护及现场技术支持，且所使用的任何相关工具必须经用户认可。

六、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；乙方未按约定期限交付标的物，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。

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。

七、解决合同纠纷的方式：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。

八、其它约定事项：

根据《中华人民共和国民法典》等相关法律规定，甲乙双方遵循平等自愿、诚实信用的原则，经友好协商，补充以下约定，以兹共同遵守：

1、信息系统检测范围：按照合同约定执行。

2、漏洞检测范围：

测试大类	测试项	测试目的
身份验证类	用户注册	检查用户注册功能可能涉及的安全问题
	弱口令	检查用户登录是否存在弱口令问题
	用户登录	检查用户登录功能可能涉及的安全问题
	修改密码	检查用户修改密码功能可能涉及的安全问题
	密码重置	检查忘记密码、找回密码、密码重置功能可能涉及的安全问题
	验证码绕过	检测验证码机制是否合理，是否可以被绕过
	用户锁定功能	测试用户锁定功能相关的安全问题
会话管理类	开启不安全的HTTP方法	测试目标系统是否开启不安全的HTTP请求方法
	Cookie重放攻击	检测目标系统是否仅依靠cookie来确认会话身份，从而易受到cookie回放攻击
	会话令牌分析	Cookie具有明显含义，或可被预测、可逆向，可被攻击者分析出cookie结构
	会话令牌泄露	测试会话令牌是否存在泄露的可能
	会话固定攻击	测试目标系统是否存在固定会话的缺陷
	跨站请求伪造	检测目标系统是否存在CSRF漏洞
访问控制类	功能滥用	测试目标系统是否由于设计不当，导致合法功能非法利用
	暗链	测试目标系统是否由于设计不当或故意设置，导致系统存在的后门或暗链
	垂直权限提升	测试可能出现垂直权限提升的情况
	水平权限提升	测试可能出现水平权限提升的情况
输入处理类	SQL注入	检测目标系统是否存在SQL注入漏洞
	文件上传	检测目标系统的文件上传功能是否存在缺陷，导致可以上传非预期类型和内容的文件
	任意文件下载	检测目标系统加载/下载文件功能是否可以造成任意文件下载问题
	XML注入	测试目标系统-是否存在XML注入漏洞
	目录穿越	测试目标系统是否存在目录穿越漏洞
	SSRF	检测目标系统是否存在服务端跨站请求伪造漏洞
	本地文件包含	测试目标站点是否存在LFI漏洞
	远程文件包含	测试目标站点是否存在RFI漏洞
	远程命令/代码执行	测试目标系统是否存在命令/代码注入漏洞
	反射型跨站脚本	检测目标系统是否存在反射型跨站脚本漏洞
	存储型跨站脚本	检测目标系统是否存在存储型跨站脚本漏洞
	DOM-based 跨站脚本	检测目标系统是否存在DOM-based跨站脚本漏洞

	服务端 URL 重定向	检查目标系统是否存在服务端 URL 重定向漏洞
	任意文件写入	检查目标系统是否存在写入任意文件执行任意系统命令漏洞
信息泄露类	error code	测试目标系统的错误处理能力，是否会输出详尽的错误信息
	Stack Traces	测试目标系统是否开启了 Stack Traces 调试信息
	敏感信息	尽量收集目标系统的敏感信息
第三方应用类	中间件	测试目标系统是否存在 jboss、weblogic、tomcat 等中间件漏洞
	CMS	测试目标系统是否存在 dedecms、phpcms 等 CMS 漏洞
操作系统类	操作系统	检测信息系统所部署服务器是否具有已公布安全漏洞

3、信息安全责任划分

（1）经乙方渗透测试结项完毕的业务系统，乙方应向甲方提交渗透测试报告，渗透测试报告应包括漏洞详情及修复建议。甲方应按照乙方提供的漏洞修复建议及业务系统实际情况，负责完成对漏洞的修复工作，乙方负责对甲方已修复的漏洞进行复测验证并编写具有法律效力的渗透测试复测报告。

（2）若甲方未对乙方提交的渗透测试报告中涉及到的信息系统漏洞进行及时修复，由此漏洞导致的安全事件由甲方承担责任。

（3）合同有效期内，乙方应根据甲方要求对郑州大学继续教育学院远程教育学院信息系统安全检测服务项目合同内指定的测试对象（信息系统）做不定期检测，通过乙方复测验证之后的信息系统如果发生安全事件，责任由乙方承担责任。

（4） 在合同指定的信息系统范围内以及合同有效期内，若因乙方在漏洞检测范围内未能检测出的安全漏洞发生的安全事件由乙方承担责任。

（5） 乙方仅对郑州大学继续教育学院远程教育学院安全检测项目合同指定的测试对象(信息系统)承担安全检测责任，乙方不承担因网络等其他支撑被测信息系统运行的软硬件平台存在的安全漏洞导致的安全事件带来的损失及责任。

（6）甲乙双方都已充分认识到网络安全是“动态的、相对的”，需要持续通过技术和管理手段来不断加强系统的安全。甲方承诺应积极配合乙方的信息系统安全检测工作，甲方完全理解乙方完成本合同项下安全检测服务需要甲方的全力支持和及时配合，且有赖于甲方提供准确、完整的信息和数据。甲方应向乙方提供并允许乙方使用为履行本合同所需的信息、数据、文档、设施、工作条件等，并确保向乙方提供的信息及数据的准确性和完整性。在服务期间，甲方应该配备

技术人员，协助乙方进行工作。

（7） 乙方出具的渗透测试报告及复测报告当中涉及的安全漏洞仅适用于乙方测试期间甲方提供的版本和运行环境。甲方系统运行环境发生变化若不及时通知乙方，乙方不承担因系统运行环境变化而引入的新的安全风险导致的安全事件的损失及责任。

（8） 在合同范围之内，乙方对甲方被测系统所遭受的以下损失不承担任何责任：

(a) 由于系统中非 CVE 漏洞导致的损失；

(b) 由于未暴露的 0day 漏洞导致的损失；

(c) 由于甲方硬件故障、链路故障或拒绝服务攻击而导致的损失。

4、安全运维体系建设

乙方在实施完成渗透测试之后，依据甲方实际网络环境，协助甲方设计适合甲方使用的 《安全运维体系建设框架方案》 。

九、本协议未尽事宜双方协商可补充之。

十、本协议书正本陆份，甲方执肆份，乙方执贰份，具有同等法律效力。

十一、本协议自签定之日起生效，随协议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

电话：67763223

开户银行：工商银行郑州中航名都支行

户名：郑州大学

帐号：1702021109014403854

签定日期：2023.3.16

乙方（盖章）：河南金盾信安检测评估中心有限公司

法定代表或代理人：

单位地址：郑州市郑东新区中道东路 6 号创意岛大厦 B 区 B620

电话：0371-55395206

开户银行：上海浦东发展银行郑州经三路支行

户名：河南金盾信安检测评估中心有限公司

帐号：76060154800006231

签定日期：2023.3.16

签约地点：郑州市