# 吉林财经大学2025等保测评及网络安全保障服务项目

# 合同书

合同编号：

采购方（甲方）：吉林财经大学

供货方（乙方）：长春市博鸿科技服务有限责任公司

签约地点：吉林财经大学

签订日期：2025.7.9

吉林财经大学需求的吉林财经大学2025等保测评及网络安全保障服务项目经吉林省中维项目管理咨询有限公司以编号为采购计划-[2025]-06381号的竞争性谈判文件在国内公开招标，评标委员会评定长春市博鸿科技服务有限责任公司为中标供应商。甲、乙双方按照《中华人民共和国民法典》和有关法律法规，遵循平等、自愿、公平和诚实信用原则，同意按照下面的条款和条件订立本合同，共同信守。

第一条合同标的：

| 序号 | 服务名称 | 服务内容 | 单位 | 数量 | 单价 | 合价 |
|---|---|---|---|---|---|---|
| 1 | 互联网资产暴露面梳理 | 详见附件：项目服务内容一览表 | 项 | 1 | 9000 | 9000 |
| 2 | 网站安全监测预警 | 详见附件：项目服务内容一览表 | 项 | 1 | 18000 | 18000 |
| 3 | 网络安全监测与处置 | 详见附件：项目服务内容一览表 | 项 | 1 | 83000 | 83000 |
| 4 | 漏洞评估服务 | 详见附件：项目服务内容一览表 | 项 | 1 | 22000 | 22000 |
| 5 | 渗透测试 | 详见附件：项目服务内容一览表 | 项 | 1 | 22000 | 22000 |
| 6 | 安全加固协助指导 | 详见附件：项目服务内容一览表 | 项 | 1 | 15000 | 15000 |
| 7 | 安全培训服务 | 详见附件：项目服务内容一览表 | 项 | 1 | 9000 | 9000 |
| 8 | 应急演练服务 | 详见附件：项目服务内容一览表 | 项 | 1 | 9000 | 9000 |
| 9 | 安全通告 | 详见附件：项目服务内容一览表 | 项 | 1 | 8000 | 8000 |
| 10 | 应急响应服务 | 详见附件：项目服务内容一览表 | 项 | 1 | 27000 | 27000 |
| 11 | 安全态势分析 | 详见附件：项目服务内容一览表 | 项 | 1 | 18000 | 18000 |
| 12 | 等保测评服务 | 详见附件：项目服务内容一览表 | 项 | 4 | 60000 | 240000 |
| 合计：¥480,000.00（大写：肆拾捌万元整） | | | | | | |

第二条质量标准

质量标准：符合国家及行业相关规定

第三条乙方承诺

1、 乙方需出具服务质量承诺函，确保合同履行期限的服务质量、违约赔偿责任等，作为甲方验收的

重要参考资料。

2、 乙方保证在合同履行期限内按甲方约定的项目内容服务。如合同约定的服务内容出现在合同履行期限内，但在合同履行期限内未完成该项服务内容的，则乙方承诺将继续完成该项服务内容。

第四条验收方式

1、合同签订后，服务开始30日内，甲方按照有关规定组织验收，验收合格后由甲方出具《验收合格单》。验收结果不合格，甲方有权要求乙方整改，直至验收合格为止。因验收不合格给甲方造成的一切损失均由乙方承担。

第五条双方责任：

1、甲方责任

①、积极配合乙方进行等保测评及网络安全保障服务工作，并提供场地及环境方面的条件；

②、按照约定按时向乙方支付款项；

③、本协议约定的其他责任。

2、乙方责任

①、合同签订后乙方做入场准备，按照合同履行期限的起始时间提前3天入场提供等保测评及网络安全保障服务；

②、按合同约定的时间和方式按时、按质提供等保测评及网络安全保障服务；

③、提供合同相应金额的增值税专用发票；

④、本协议约定的其他责任。

第六条付款方式及期限

1、本合同由甲方自筹资金，由甲方根据发票、《验收合格单》、采购合同等手续自行支付。验收合格后30日内支付（如遇封账、审计等特殊情况，付款期限顺延）合同金额的100%。

2、乙方收款账户：

收款单位：长春市博鸿科技服务有限责任公司

收款账号：0126011000005502

开户行名称：吉林银行长春高新开发区支行

第七条履约保证金

1、履约保证金金额为：人民币贰万肆仟元整（¥24000.00 ），乙方应在签署合同之前向甲方缴纳合同总价5%的履约保证金。

2、支付方式：转账支付至甲方如下账户：

名称:吉林财经大学

开户行:吉林九台农村商业银行股份有限公司新嘉支行

账号:071043101101520000 11710

3、保证范围：乙方按合同的约定应履行的全部义务。

4、履约保证金的退回：如乙方如约履行采购合同，甲方在验收合格后 20 个工作日内将履约保证金采用银行转账方式无息退回。如乙方违反合同约定的义务，甲方有权在履约保证金中直接扣除乙方应向甲方支付的违约金或损失赔偿额，如有不足的，由乙方另行承担赔偿责任。

第八条违约责任

1、乙方所提供服务不符合合同规定标准的，依据《服务质量承诺函》甲方有权拒绝，且乙方应向甲方偿付合同总价款 30%的违约金。如违约金不足以偿付给甲方造成的损失，则违约金以甲方实际损失为准。

2、甲方未按合同约定的时间付款的，每逾期一日，按应付而未付款项总额的 1‰向乙方支付违约金，违约总金额不超过未支付部分金额的 20%。

第九条解决争议的办法

在合同签订、履行过程中发生争议的，双方应当本着友好、协作的精神进行协商；协商不成，提起诉讼的，双方同意由甲方所在地人民法院管辖。

第十条合同构成

1、合同构成：下列文件构成本合同不可分割的组成部分，与本合同具有同等法律效力；

1.1 本合同书；

1.2 招标文件及澄清、修改、补遗文件；

1.3 乙方投标和报价文件、中标通知书及书面澄清、说明、补正文件；

1.4 合同的其他附件。

第十一条其它

1.合同份数：本合同一式四份，甲乙双方各执二份，具有同等法律效力。

2.合同生效：本合同在甲乙双方法定代表人或其授权代表签字并加盖公章之日起生效。

3.合同修改：除甲乙双方签署书面修改、补充协议外，本合同条件不得有任何变化或修改。

甲方：吉林财经大学

地址：长春市净月大街 3699 号

法定代表人

（或授权代表）：

日期：2025.7.9

乙方：长春市博鸿科技服务有限责任公司

地址：长春市净月开发区天普路以南，生态大街以西长春总部基地金融十六院 7#办公楼 101 号

法定代表人

（或授权代表）：张建

日期：2025.7.9

（以下为附件）

## 附件：项目服务内容一览表

| 序号 | 服务名称 | 服务内容 | 单位 | 数量 | 单价 | 合价 |
|---|---|---|---|---|---|---|
| 1 | 互联网资产暴露面梳理 | 1.通过大数据挖掘和调研的方式确定互联网资产范围，基于 IP 或域名，采用网络扫描、搜索引擎等多种探测技术，对相关资产暴露在互联网上的业务系统、主机/服务器、安全设备、网络设备等进行主动发现，并形成资产及应用列表及报告，提前发现可能存在的安全隐患，并遵循最大化收敛，最小化暴露原则减少互联网资产暴露面，减少受攻击面，提升网络安全性。<br>2.项目参与人 2 名中级工程师，具备中国信息安全测评中心颁发认证的工程师，以攻击者视角，通过模拟黑客攻击的方式，帮助客户梳理暴露在互联网侧的资产，并进行安全性测试。检测安全风险隐患，评估安全防护水平，量化安全风险，针对风险问题给出合理化整改建议。<br>提供不少于 2 次的互联网资产暴漏面梳理。<br>交付《互联网资产梳理报告》 | 项 | 1 | 9000 | 9000 |
| 2 | 网站安全监测预警 | 1.定期为门户网站首页进行网站结构分析、漏洞分析，用户无需采购任何 Web 应用扫描产品，即可获知网站的漏洞情况，以及修补建议。<br>2.提供 7*24 小时远程事件值守服务，包括挂马、黑链、篡改、敏感内容监测。<br>3.实时监测服务站点的页面情况，识别网站页面隐藏的恶意代码，避免由于网站被挂马所带来的不良影响。<br>4.实时监测服务站点是否出现一些敏感关键字，如果发现敏感内容，在第一时间通知。<br>5.实时监测服务站点页面状况，发生页面被篡改情况，第一时间通知采购人，避免页面篡改所造成的声誉和法律风险。全年提供。<br>6.项目参与人 1 名中级工程师，具备中国信息安全测评中心颁发认证的工程师，对报告结果进行分析验证，综合评估影响范围、程度等。<br>交付《网站安全监测服务报告》 | 项 | 1 | 18000 | 18000 |
| 3 | 网络安全监测与处置 | 能够获得权威第三方国家计算机网络与信息安全管理中心吉林分中心技术支持，利用国家网络安全监测技术手段对以下服务开展 7*24 小时监测预警通报：<br>1.网络钓鱼监测处置服务<br>针对网站、在线支付系统等在线服务系统的仿冒和网络钓鱼事件监测。<br>2.DDos 监测溯源服务<br>在全网范围内，对针对分布式拒绝服务攻击等流量异常事件进行监测。<br>3.域名安全监测处置服务<br>及时发现域名劫持、域名恶意指向等域名安全事件。 | 项 | 1 | 83000 | 83000 |

| 序号 | 服务名称 | 服务内容 | 单位 | 数量 | 单价 | 合价 |
|---|---|---|---|---|---|---|
| | | 4.联网终端安全监测服务<br>对单位接入互联网的终端和信息资产感染木马、蠕虫、僵尸程序等恶意程序事件进行监测、预警通报并协助处置。<br>交付《网络安全监测报告》 | | | | |
| 4 | 漏洞评估服务 | 1.对项目中涉及的网络设备、安全设备、数据库、中间件、虚拟机、操作系统和业务系统等进行安全漏洞扫描、用户名及口令猜测检查，及时发现最新的安全漏洞及风险隐患分布情况，并出具详细的漏洞扫描报告及修复建议，提高信息系统安全性，并掌控信息系统整体的安全态势。<br>2.为避免同一品牌的漏洞扫描产品造成检查结果具有单一性，需要提供两种不同制造厂生产的漏洞扫描产品进行交叉扫描检查验证，以减少误报及漏报率，提升扫描结果准确性，确保所有业务系统均能安全运行。<br>3.项目参与人至少 1 名中级和 1 名初级工程师，具备中国信息安全测评中心颁发认证的工程师，对报告结果进行分析验证，综合评估影响范围、程度等。<br>提供 4 次的漏洞评估服务。<br>交付物：《安全漏洞扫描报告》 | 项 | 1 | 22000 | 22000 |
| 5 | 渗透测试 | 综合利用安全扫描工具、漏洞利用工具、人工渗透测试（黑盒测试）等手段，采用外部渗透方式对应用系统和网络安全基础设施进行非破坏性质的模拟入侵者攻击的测试，检测外部威胁源和路径，发现网络和业务系统中存在的安全缺陷，提供渗透测试报告和改进建议，并且为修补漏洞、抵御安全风险提供技术支持。<br>渗透测试方法及漏洞挖掘情况根据系统自身存在的漏洞而定，包括但不限于以下内容:<br>1.在服务过程中提供渗透测试工具，渗透测试工具有快速检测、WEB 应用测试、资产发现、漏洞检测与验证等功能。<br>2.工具支持内网渗透、HTTP 隧道、Socks 隧道、数据库管理、内置常用 POC 库（常用漏洞 POC 数量 700 及以上）、内置常用 EXP 库（包含 Shiro、各类 OA、Struts2、K8_Struts2、weblogic、tomcat 等）。<br>3.Web 层安全渗透：SQL 注入、任意文件上传、跨站脚本攻击（XSS）、XML 外部实体（XXE）注入、跨站点伪造请求（CSRF）服务器端请求伪造（SSRF）、任意代码执行、HTTP 明文传输、命令执行注入等；<br>4.业务逻辑安全渗透：未授权访问、验证码缺陷、反序列化命令执行、用户名枚举、用户弱口令、平行越权访问、垂直越权访问、业务逻辑漏洞等；<br>5.中间件安全渗透：中间件配置缺陷、中间件弱口令、Jboss 反序列化命令执行、Jenkins 反 | 项 | 1 | 22000 | 22000 |

| 序号 | 服务名称 | 服务内容 | 单位 | 数量 | 单价 | 合价 |
|---|---|---|---|---|---|---|
| | | 序列命令执行、Webloigc 反序列化命令执行、Apache Tomcat 样例目录 session 操纵等；<br>6.服务器安全测试：操作系统弱口令、数据库弱口令、本地权限提升、数据库信息探测、永恒之蓝、windows 操作系统漏洞等。<br>7.项目参与人 2 名中级工程师，具备中国信息安全测评中心颁发认证的工程师，掌握 web 攻击和内网渗透相关漏洞原理和工具的使用，掌握 web 攻击和内网渗透相关工具和攻击行为的检测方法，能站在威胁检测的角度赋能相关产品和核心技术，提升威胁检出率。<br>提供 4 次渗透测试服务。<br>交付《渗透测试报告》 | | | | |
| 6 | 安全加固协助指导 | 1.根据漏洞扫描、安全检测、日志分析和配置检测等相关检查结果中发现的问题，结合客户安全合规方面的要求，协调并指导服务器、网络设备、数据库系统等有关厂商进行修补，加强安全配置、安全加固处理，及时对授权期内的安全设备进行规则库升级、系统升级等工作，根据业务需要修改、优化安全设备的策略、规则等，并完成复查工作。<br>2.根据实际需求调整现有安全设备的规则、策略，关闭或卸载设备上不必要的服务和应用程序，减少资源占用。优化网络路由，减少数据传输延迟。<br>3.项目参与人 2 名中级工程师，具备中国信息安全测评中心颁发认证的工程师，能够协助相关方实施计划以及完成整改实施，加固必须事前有方案、过程有记录、异常有报告。<br>全年提供。<br>交付《安全加固方案》、《安全加固报告》 | 项 | 1 | 15000 | 15000 |
| 7 | 安全培训服务 | 通过课件分析讲解、安全技术演示、安全攻防操作等方式对办公人员及业务使用者进行安全意识教育培训及安全技术培训，客户可根据自身需求选择适合的培训内容，具体如下：<br>1.安全意识培训：针对目前主流的网上诈骗、个人信息泄露、办公安全意识等进行全面的讲解，提升人员安全意识，满足等保建设与合规性建设要求，防止黑客通过安全意识薄弱的人员采取钓鱼、社工等方式带来攻击事件。<br>2.安全技术培训：结合业务特性，针对目前主流安全技术和常用的安全技能进行安全技术培训，使用户了解安全设备作用和使用、安全风险识别方法、漏洞防护技术、病毒防护等知识。<br>3.定制化安全培训：按照客户需求和实际情况组织的专题交流研讨以及定制化培训，提升网络安全意识，了解安全技术能力及信息安全管理体系的基础知识，使组织切实的执行和贯彻安全的管理，提升组织的核心竞争力。<br>4.项目参与人 1 名中级工程师，具备中国信息 | 项 | 1 | 9000 | 9000 |

| 序号 | 服务名称 | 服务内容 | 单位 | 数量 | 单价 | 合价 |
|---|---|---|---|---|---|---|
| | | 安全测评中心颁发认证的工程师，了解网络安全相关的法律法规及政策标准，具有一定的培训授课经验，优秀的沟通表达能力，能清晰传达网络安全知识和操作技巧。<br>每年 1 次。<br>交付《培训方案》、《培训讲义》 | | | | |
| 8 | 应急演练服务 | 1.通过设定发生的安全事件而进行的以检验用户应急预案和应急流程的经济性、合理性和可操作性，评估各方面人员应对安全突发事件的组织指挥能力和应急处置能力，提高应急人员应急工作熟练程度，提升全员安全意识，结束后编制应急演练报告。<br>2.根据实际环境，提供专项预案，准备演练场景，以模拟演练的方式检验应急预案和应急流程是否完善，提高应急处理能力，场景应包含但不限于数据安全、钓鱼邮件、勒索病毒等。<br>3.项目参与人至少 2 名中级工程师，具备中国信息安全测评中心颁发认证的工程师，掌握网络安全事件的应急响应流程，能够快速对安全事件进行响应和处理，具有一定的网络安全领域实践经验，尤其是参与过网络安全事件应急响应或攻防演练的经验<br>每年 1 次。<br>交付《应急演练方案》、《应急演练报告》 | 项 | 1 | 9000 | 9000 |
| 9 | 安全通告 | 1.及时通告国内外安全机构及漏洞发布平台发布的相关安全漏洞，并提供相应修补方案，及时把握国内外网络安全现状与态势，了解网络安全技术发展方向，及时消除企业网络安全漏洞与隐患，避免引发网络安全事件进而对形象造成影响。<br>2.针对特殊或突发情况，同时提供“紧急安全漏洞通告”和“紧急安全威胁通告”。安全事件通告服务收集、整理、维护、发布的专项预警类服务。<br>3.项目参与人 2 名中级工程师，具备中国信息安全测评中心颁发认证的工程师，熟悉渗透测试和漏洞验证能力，能够对通告内容进行有效验证，并筛选出与业务系统、安全设备、操作系统等相关的通告内容。<br>全年提供。<br>交付《安全通告》 | 项 | 1 | 8000 | 8000 |
| 10 | 应急响应服务 | 1.帮助客户完成应用服务瘫痪问题、网络阻塞、DDoS 攻击问题 、服务器遭劫持问题、系统异常宕机问题、恶意入侵、黑客攻击问题、恶意入侵、黑客攻击问题、病毒爆发问题、内部安全事故等安全事件的应急响应技术响应指导，出具应急响应服务报告，7×24 小时的应急响应技术支持服务，当网络安全出现状况时，能够第一时间进行响应，配合用户将危险降到最低。<br>2.响应流程：在收到事件告警后，15 分钟内进 | 项 | 1 | 27000 | 27000 |

| 序号 | 服务名称 | 服务内容 | 单位 | 数量 | 单价 | 合价 |
| --- | --- | --- | --- | --- | --- | --- |
| | | 行故障事件的鉴别，如果是安全事件，则立即启动应急响应服务流程，如果不是安全事件，立即回复相关人员，并建议寻求其他方面的支持应急响应服务事件处理流程主要分为三个阶段，包括事件初期、应急响应实施及输出报告与汇报：应急响应服务事件处理流程主要分为三个阶段，包括事件初期、应急响应实施及输出报告与汇报。<br>3.服务方式：应提供现场服务和远程服务，现场服务方式为：接到校方紧急服务请求，投标方支持人员在最短时间内赶赴客户现场，协助校方分析事件可能的原因，解决各类安全事件；远程服务为指通过电话、QQ 远程协助、远程临时接入等非现场的活动，协助校方分析事件可能的原因，解决各类安全事件。<br>4.响应时间：对于一般事件首先采取安全咨询的方式帮助用户自行解决，当校方安全管理员经过努力无法自行解决时，指派工程师将采用应急响应服务通过远程或本地服务方式帮助用户解决安全事件；对于严重事件，将启用应急响应服务，在 2 个小时内（另加上路程时间）到达用户现场，采用本地服务方式帮助用户处理安全事件；对于紧急事件的处理，承诺在一个小时内（另加路程时间）到达校方现场，采用安全应急响应服务流程为用户尽快解决紧急安全事件。<br>5.事件紧急程度划分：紧急事件为校方提供业务的系统由于安全原因崩溃、系统性能严重下降，已无法提供正常服务。本地区出口路由由于网络安全原因非正常中断，严重影响用户使用。公众服务由于安全原因停止服务或者造成恶劣影响的；严重事件为用户内部的业务支持系统由于安全事件出现问题，导致不能运转正常不稳定。部分服务由于安全原因中断，影响用户正常使用<br>一般事件为由于安全原因导致系统出现故障，但不影响用户正常使用。校方提出安全技术咨询、索取安全技术资料、技术支援等。<br>6.项目参与人 2 名中级工程师，具备中国信息安全测评中心颁发认证的工程师，熟练使用防火墙、IDS/IPS、WAF、漏洞扫描工具等安全设备，具备日志分析及安全加固能力，能够实时监控网络流量，快速识别异常行为并启动应急响应流程，具备安全事件分析能力。<br>全年提供。<br>交付《应急响应报告》 | | | | |
| 11 | 安全态势分析 | 1.结合各项服务内容，结合校方现有安全监测手段，综合评估当前校园网网络安全态势，分析各类安全日志，挖掘潜存的网络安全威胁，从攻击手段、漏洞利用、攻击者信息、受攻击者信息、事件发生频率等多个维度开展安全态 | 项 | 1 | 18000 | 18000 |

| 序号 | 服务名称 | 服务内容 | 单位 | 数量 | 单价 | 合价 |
|---|---|---|---|---|---|---|
| | | 势分析工作。<br>2.项目参与人1名中级和1名初级工程师，具备中国信息安全测评中心颁发认证的工程师，熟练使用防火墙、IDS/IPS、WAF、漏洞扫描工具等安全设备，具备渗透测试及日志分析，能够实时监控网络流量，快速识别异常行为并启动应急响应流程，具备安全事件分析能力。<br>交付《网络安全月报》。 | | | | |
| 12 | 等保测评服务 | 对人事系统（二级）、本科生教务管理系统（二级）、门户网站系统（二级）、学工系统（二级）上述信息系统进行等保测评。<br>（1）测评准备阶段<br>系统调研：对信息系统进行资料收集和系统调研；进行信息收集、工具准备，编制测评计划书、调查问卷收集等。<br>输出结果：测评计划书、测评启动会汇报、调研结果报告、工具及表单准备。<br>（2）测评方案编制阶段<br>测评方案编制：方案编制、测评对象确认、测评指标确认、测评内容确认、整体测评方法确认、风险分析方法确认、开发指导书、编制结果记录表等，要求中标人在签订合同后出具相关方案。<br>输出结果：测评方案、测评指导书、结果记录表。<br>（3）现场测评阶段<br>现场测评：通过访谈、检查、测试、分析等方法，现场根据测评指导书对信息系统进行现场测评并进行结果证据收集确认。<br>输出结果：现场测评结果记录表。<br>（4）报告编制阶段<br>安全需求分析：依据单元测评结果汇总进行整体测评分析、风险分析、结果汇总、结论形成、结果判定、整改建议等。<br>输出结果：单项、单元评估结果汇总，等级测评报告。<br>依据《吉林省网络安全等级保护测评机构管理办法（试行）》第十五条，按照统一模板出具测评报告。 | 项 | 4 | 60000 | 240000 |
| 合计：**¥480,000.00**（大写：肆拾捌万元整） | | | | | | |